Citation 1

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/16, 12/66, H04Q 7/00, 7/24

A1

(11) International Publication Number: WO 00/08803

(43) International Publication Date: 17 February 2000 (17.02.00)

(21) International Application Number: PCT/US99/16791

(22) International Filing Date: 23 July 1999 (23.07.99)

(30) Priority Data:
09/128,553 3 August 1998 (03.08.98) US

(71) Applicant: OMNIPOINT TECHNOLOGIES III, INC. [US/US]; 1365 Garden of the Gods Road, Colorado Springs, CO 80907 (US).

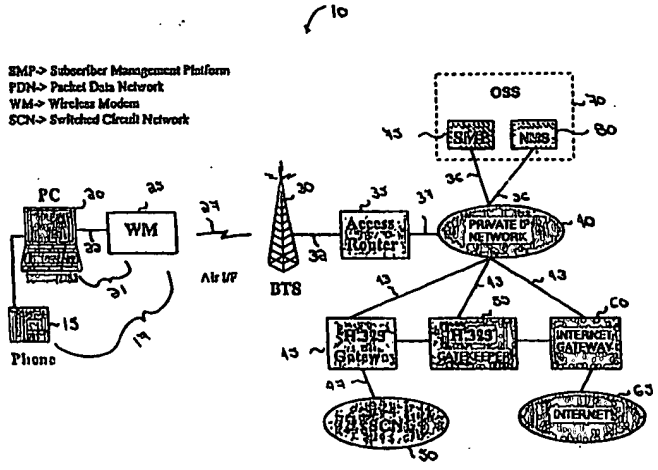
(72) Inventors: APFEL, Patrick, R.; 2 Berthe Circle, Colorado Springs, CO 80906 (US). SOLA, Ismail, E.; 5145 Seven Oaks Drive, Colorado Springs, CO 80919 (US). MENON, Narayan, P.; 5910 Bay Springs Lane, Colorado Springs, CO 80918 (US). BILGIC, Izzet, M.; 6841 Goldcrest Court, Colorado Springs, CO 80919 (US). LEDSHAM, Stephen, D.; 975 Pulpit Rock Circle South, Colorado Springs, CO 80918 (US).

(74) Agent: LYON & LYON LLP; McKernan, Lynn, Y., Suite 4700, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A PLUG AND PLAY WIRELESS ARCHITECTURE SUPPORTING PACKET DATA AND IP VOICE/MULTIMEDIA SERVICES



(57) Abstract

A telecommunications network (10) supporting wireless access to one or more public packet data networks, including, but not limited to, the Internet, and to one or more public switched circuit networks, for example, but not limited to, e.g., the public system telephone network (PSTN). A computing device and a computing device/voice access device combination each comprise subscriber equipment (21). The wireless access (35) network supports both switched circuit transmissions and packet data transmissions to one or more network subscribers, via respective network subscriber equipment (21). The wireless access (35) network comprises a protocol for packet data message transmissions from a public data network, including, but not limited to, the Internet (65), to a network subscriber. The wireless access (35) network also comprises a protocol (40) for voice message transmissions from a switched circuit network to a network subscriber.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Description
A Plug And Play Wireless Architecture Supporting Packet Data And IP Voice/Multimedia Services

Field of the Invention

A telecommunications system, and, more specifically, a system supporting wireless access to public data networks and public switched circuit (telephony) networks.

Description of the Technology

Generally, known telecommunication systems that have attempted to provide both packet data and voice services have used the concept of an overlay network. More specifically, in known communication systems, a network supporting packet data has been overlaid on top of an already existing base system that supports voice. In this manner, voice and packet data transport, i.e., transmissions, follow separate paths beyond a point in the network, e.g., from a base station onwards.

Known systems transmit voice in a circuit-switched mode and packet data in a packet switched mode. In packet switched mode, information is sent in many sections, or packets, over one or more physical transmission routes, and is thereafter re-assembled at the receiving end. Because information is sent in packets, transmission resources, e.g., physical transmission interfaces, can be shared among more than one user and/or among more than one data stream at a time.

In contrast, in circuit-switched mode, there is generally a single, unbroken connection between the sender and the receiver of the voice stream, or transport. In circuit-switched mode, a voice transport is not divided and transmitted in sections, and, thus, once a transmission connection is made to a network, e.g., as for a telephone call, even if there is no voice transport at a particular time, e.g., when a call is on hold, the physical connection remains exclusively dedicated to that transmission, to the exclusion of all other users of the system.

Thus, in known telecommunication systems that attempt to support both packet data and voice, generally resources are either dedicated to packet data support or, alternatively, they are dedicated to voice support. Moreover, in such known systems, resources may be consumed by voice support, to the exclusion of packet data. Too, such systems do not integrate packet data and voice support throughout the system, and thus, require the addition of resources to support the

added servic , e.g., packet data, which is overlaid on the original base system, e.g., voice.

Further, because known systems are switched circuit, i.e., voice, centric, generally end-to-end circuits are assigned for both voice and packet data transmissions. This reduces the flexibility of the system to handle multiple users accessing both switched circuit and packet data services at the same time. Further, such systems have no capability for supporting a "best transmit path" between various sub-components in the network in an end-to-end communication. In such systems, a single communication path, end-to-end, is established for a communication flow, voice or data. Alternative paths between components of the network that could provide better quality or faster transmission for a particular message, voice or data, are not explored or utilized in these systems.

Thus, it would be advantageous to provide an integrated, flexible wireless system that supported both packet data and voice. Further, it would be advantageous to provide an integrated voice/packet data system based on the Internet protocols, that supported equivalent message flow handling for voice and packet data throughout the network. Too, it would be advantageous to provide an integrated voice/packet data system that supported cost-effective packet data services, e.g., for Internet access, and cost-effective switched circuit services, e.g., for access to existing switched circuit (telephony) networks.

Summary Of The Invention

The inventions provide apparatus and mechanisms for furnishing, in an end-to-end fashion, a telecommunications system supporting wireless access that can handle both packet data and voice transmissions.

In a presently preferred embodiment, a voice access unit and a computing unit are connected to a radio unit that itself provides over-the-air access to a wireless access network. The wireless access network, for its part, provides access to one or more packet data networks and to one or more switched circuit networks.

The computing device is capable of receiving packet data. The voice access device is capable of receiving a voice message. The voice access device is connected to the computing device in order to receive a voice message transmitted from the wireless access network.

In a presently preferred embodiment, the wireless access network supports both switched circuit message transmissions and packet data message transmissions to a subscriber of the network. The wireless access network

comprises a protocol for packet data message transmissions from a packet data network to a subscriber. The wireless access network also comprises a protocol for voice message transmissions from a switched circuit network to a subscriber.

The wireless access network also supports a protocol for security management of the wireless access network. The wireless access network further comprises a protocol for the management of subscriber information, including, but not limited to, subscriber requested services supported by the wireless access network. The wireless access network also comprises a protocol for managing the billing of the subscribers of the network.

Therefore, a general object of the inventions is to provide a telecommunications system that supports access to both packet data services and voice services. A further general object of the inventions is to provide a cost-effective seamless wireless access network for handling both packet data and voice transports, or transmissions. Other and further objects, features, aspects and advantages of the inventions will become better understood with the following detailed description of the accompanying drawings.

Brief Description Of The Drawings

Figure 1 depicts the services of a wireless access network.

Figure 2 is a presently preferred embodiment wireless access network.

Figure 2A is a presently preferred embodiment of a Customer Premises Radio Unit (CPRU) in a wireless access network.

Figure 3 depicts the transmission interface and procedures executed between an H.323 gatekeeper and an H.323 endpoint.

Figure 4 depicts the IP voice procedures supported by a wireless access network.

Figure 5 is an alternative embodiment wireless access network.

Figure 6 depicts the centralized management operations of a wireless access network.

Figure 7 depicts the Subscriber Management Platform procedures supported by a wireless access network.

Figure 8 depicts the terminal authentication network elements in a wireless access network.

Figure 9 depicts the communication protocol planes in a wireless access network.

Figure 10 depicts the packet data signaling plane procedures supported by a wireless access network.

Figure **11** depicts the voice signaling plane procedures supported by a wireless access network.

Figure **12** depicts the protocol stacks for the packet data signaling plane in a wireless access network.

Figure **13** depicts the Terminal Management Protocol procedures supported by a wireless access network.

Figure **14** depicts the protocol stacks for the packet data bearer plane in a wireless access network.

Figure **15** depicts the protocol stacks for the voice signaling plane in a wireless access network.

Figure **16** depicts the protocol stacks for the voice bearer plane in a wireless access network.

Figure **17** depicts the Logical Link Control procedures supported in a wireless access network.

Figure **18** depicts the protocol stacks for management of a network node in a wireless access network.

Figure **19** depicts a hierarchy of management platforms within the management system of a wireless access network.

Figure **20** depicts the management of base stations and Customer Premise Radio Units (CPRUs) by a general purpose wireless access management platform of a wireless access network.

Figure **21A** depicts the protocol stacks for a base station management protocol plane.

Figure **21B** depicts the protocol stacks for a Customer Radio Unit management protocol plane.

Figure **22** depicts the network component structure for end-to-end packet bearer transmissions in a wireless access network.

Figure **23** depicts the network component structure for end-to-end signaling transmissions for authentication and subscriber management in a wireless access network.

Figure **24** depicts the network component structure for end-to-end network management signaling transmissions for node and accounting management in a wireless access network.

Description Of The Preferred Embodiments

A presently preferred embodiment of a wireless access network, or system, comprises a variety of services 1, as shown in Figure 1, for supporting wireless

access voice and data transmission functionality. More specifically, a presently preferred embodiment of a wireless access network comprises services 1 for supporting wireless access to one or more data networks, for example, but not limited to, e.g., a public data network, including the Internet, and to one or more switched circuit networks, for example, but not limited to, e.g., the public system telephone network (PSTN). The services 1 of the wireless access network include, but are not limited to, packet data services 2, voice services 3, fax services 4, security services 5, network management services 6, subscriber management services 7 and billing services 8.

Packet data services 2 of the wireless access network, include, but are not limited to, point-to-point and point-to-multipoint services. A point-to-point packet data service is a connectionless service of the datagram type, i.e., the messages are generally transferred on an unsecure transmission channel, comprising the functionality for the transmission of one or more packets of data from a single packet data network, for example, but not limited to, e.g., the Internet, to a single network subscriber, i.e., end user of the wireless access network. In the alternative direction, the point-to-point packet data service comprises the transmission of one or more packets of data from a single network subscriber to a single packet data network.

In a presently preferred embodiment a wireless access network subscriber terminal for the receipt or transmission of packet data comprises a personal computer (PC) and a wireless modem (WM). In an alternative embodiment, a terminal for the receipt or transmission of packet data comprises any computing device, for example, but not limited to, e.g., a personal computer (PC), a smart terminal, a palm pilot or a work station, and a radio unit, for example, but not limited to, e.g., a wireless modem (WM).

In a second presently preferred embodiment, a wireless access network subscriber terminal comprises one or more personal computers (PCs) and a Customer Radio Premises Unit (CPRU). In an alternative of this second presently preferred embodiment, a terminal for the receipt or transmission of packet data comprises one or more of a variety of computing devices, including, but not limited to, e.g., a personal computer (PC), a smart terminal or a work station, and a CPRU.

In a presently preferred embodiment, each packet data transmission is ind pendent of the preceding and succe ding packet data transmissions. In a presently preferred embodiment, on the radio, i.e., wireless, or over-the-air, transmission interface of the wireless access network, the point-to-point packet

data service utilizes an acknowledge transfer m chanism for reliable wireless transmission and reception. In a presently preferred embodiment, the network layer protocol for the point-to-point connectionless packet data service is the Internet Protocol (IP).

A point-to-multipoint packet data service comprises the functionality for the transmission of messages between participants of an internet protocol multicast (IP-M) group. A point-to-multipoint packet data service is a connectionless service of the datagram type, i.e., the messages are generally transferred on an unsecure transmission channel, comprising the functionality for the transmission of one or more packets of data from a single packet data network, for example, but not limited to, e.g., the Internet, to two or more network subscribers.

Participation in and data transfer in the point-to-multipoint service also relies on the Internet Protocol (IP).

Voice services 3 of the wireless access network comprise the establishment, maintenance and release of outgoing voice calls between a subscriber of the wireless access network and another subscriber or a switched circuit network supported by the wireless access network. In a presently preferred embodiment an H.323 terminal for IP packet voice receipt or transmission comprises a telephone, a personal computer (PC) and a wireless modem (WM). In an alternative embodiment, an H.323 ter.ninal for the receipt or transmission of IP packet voice comprises any voice access device, for example, but not limited to, e.g., a telephone, any computing device, for example, but not limited to, e.g., a personal computer (PC), a smart terminal, a palm pilot or a work station, and a radio unit, for example, but not limited to, e.g., a wireless modem (WM).

In a second presently preferred embodiment, an H.323 terminal for IP packet voice receipt or transmission comprises a telephone and a Customer Radio Premises Unit (CPRU). In an alternative of this second presently preferred embodiment, an H.323 terminal for the receipt or transmission of IP packet voice comprises any voice access device, for example, but not limited to, e.g., a telephone, and a CPRU.

In a presently preferred embodiment, voice services are based on the H.323 protocol standard, overlaid on the Internet Protocol (IP) based underlying packet data services 2. In a presently preferred embodiment, voice messages are transmitted within the wireless access network in an IP packet datagram format.

Fax services 4 of the wireless access network are supported via the Internet Protocol (IP) based underlying packet data services 2, and provide a mechanism for the transmission and receipt of fax-based messages.

Security services 5 of the wireless access network support security features including, but not limited to, subscriber authentication, terminal authentication, user identity confidentiality and user information confidentiality. Subscriber authentication and terminal authentication provide network confirmation that the respective subscriber and terminal identities being used are proper, i.e., that the respective subscriber on the respective terminal is actually as claimed in the request for network services. Subscriber and terminal authentication procedures protect the network against unauthorized use and against the impersonation of authorized users.

User identity confidentiality provides identity privacy for subscribers using the radio, i.e., wireless, or over-the-air, resources of the wireless access network. User identity confidentiality includes, but is not limited to, providing protection against tracing the location of a subscriber of the network by listening to, or otherwise intercepting, signaling exchanges on the network's wireless interface.

User information confidentiality, includes, but is not limited to, encryption, and subsequent decryption, of messages, both voice and data, transmitted on the network. User information confidentiality provides the mechanism for protecting the confidentiality of messages, voice and data, that are transmitted over the network's wireless interface.

The security services 5 of the wireless access network support a combination of techniques for ensuring that the public entry points to the wireless access network are protected against unauthorized access. The security services 5 also support functionality to prevent the unauthorized access and use of network nodes, or elements, for example, but not limited to, base stations, access routers, gateways and gatekeepers.

In a presently preferred embodiment, one technique for achieving both secure network services and secure network node management comprises access authentication based on base station fire walling. With this technique, unauthorized users are prevented by the base stations of the wireless access network from accessing the remainder of the network. Gateway fire walling is also employed for preventing unauthorized access to the wireless access network via external networks, e.g., via external packet data or external switched circuit networks supported by the wireless access network. Data origin authentication procedures are executed as additional security measures for securing the network node management functionality.

Network management services 6 of the wireless access network manage the network elements, or nodes, that comprise the wireless access network, for

example, but not limited to, base stations, access routers, gateways, and gatekeepers. The network management services 6 support management functions including, but not limited to, configuration management, fault management, performance management and accounting management.

Subscriber management services 7 of the wireless access network support the management of subscriber profiles. A subscriber profile includes, but is not limited to, subscription information on services and other parameters that have been assigned to an end user, i.e., subscriber, of the network for an agreed contractual period. In a presently preferred embodiment, a subscriber profile comprises a respective subscriber, or customer, identification, the subscribed for network services and a quality of service (QoS) level assigned to the respective subscriber.

In a presently preferred embodiment, a particular service request may be validated against the respective subscriber's subscription profile. For example, if a subscriber has contracted for packet data services only, then a packet data request from the subscriber will be validated, and subsequently executed, by the network. However, a voice request from the subscriber will be invalidated, as voice services are not present in the subscriber's subscription profile because they have not been contracted for by the subscriber. Thus, a voice request from the subscriber will not be executed by the network.

Billing services 8 of the wireless access network comprise mechanisms for charging a subscriber, i.e., an end user of the network, for wireless access, for packet data services, for example, but not limited to, e.g., Internet access, and for voice services. In a presently preferred embodiment, a centralized billing system is used to consolidate subscriber billing for all provided services.

The wireless access service is a fundamental wireless network service without which the other services can not be provided. In a presently preferred embodiment, the mechanism for charging for wireless access is a flat rate pricing strategy based on a peak throughput level selected by the subscriber.

Flat rate pricing for wireless access is attractive as subscribers are already accustomed to paying flat rate prices for access to traditional information and communication systems, e.g., a local telephone company providing public switched telephone network (PSTN) access. Further, a simple network architecture can support flat rate pricing for wireless access.

However, the personal communications system (PCS) radio, i.e., over-the-air, spectrum is a limited resource. Thus, in a presently preferred embodiment, different flat rate charges are associated with a number of subscriber-requested

quality of service (QoS) levels. This billing scheme for wireless access protects the wireless resources from over use, without a requisite need for a complex usage-based billing scheme.

Packet data service support is a subscriber option. In an embodiment, the mechanism for charging for packet data services is a flat rate scheme. In an alternative embodiment, the mechanism for charging for packet data services is a usage-based scheme. In yet another alternative embodiment, the mechanism for charging for packet data services is a combination flat rate and usage-based scheme. In a presently preferred embodiment, the Remote Authentication Dial In User Service (RADIUS) accounting protocol is used for the transfer of accounting information, for, but not limited to, billing purposes, between an external data network, e.g., the Internet, access server entity and the wireless access network's centralized billing system.

Voice service support is also a subscriber option. In a presently preferred embodiment, the mechanism for charging for voice services is based on the scheme used by traditional telephony systems, i.e., based on the call duration and the called party destination address.

In a presently preferred embodiment, the wireless access network supports terminal transportability. In a presently preferred embodiment, a terminal comprising a wireless modem can change its point of attachment, i.e., its physical hook-up location, to the network, and thereafter continue to transmit and receive messages, voice, data and signaling.

A presently preferred embodiment of a system, or network, 10 for supporting wireless access to one or more external data networks, for example, but not limited to, e.g., the Internet, and to one or more external switched circuit networks, for example, but not limited to, e.g., the public system telephone network (PSTN), is shown in Figure 2. In a presently preferred embodiment, the network 10 comprises a wide area network (WAN). In a presently preferred embodiment, the system 10 comprises three sub-networks.

The first sub-network is a core packet data network. In a presently preferred embodiment, the core packet data network is comprised of one or more computing devices 20, for example, but not limited to, personal computers (PCs), smart terminals, palm pilots, work stations, or any combination thereof. In a presently preferred embodiment, the core packet data network is also comprised of one or more radio units, for example, but not limited to, e.g., wireless modems (WMs) 25. In a presently preferred embodiment, a network subscriber terminal 21, or just terminal, comprises a PC and a WM 25.

In a presently preferred embodiment, the core packet data network also comprises one or more base transceiver stations (BTSs) 30, also referred to as base stations, and one or more access routers 35. In a presently preferred embodiment, the core packet data network also comprises an Internet Protocol (IP) network 40, for example, but not limited to, e.g., a private IP network, a packet data gateway, including an Internet gateway 60, and one or more packet data networks, including, the Internet 65.

The second sub-network of the system 10 is an Internet Protocol (IP) packet voice network. In a presently preferred embodiment, the IP packet voice network comprises one or more voice access devices, for example, but not limited to, telephones 15, one or more computing devices 20, for example, but not limited to, e.g., PCs, one or more radio units, for example, but not limited to, e.g., wireless modems (WM) 25, a gateway 45, a gatekeeper 55, and one or more external switched circuit networks (SCN) 50. In a presently preferred embodiment, a telephone, a PC and a WM 25 comprise an H.323 terminal 17, i.e., a terminal capable of supporting IP packet voice services. In a presently preferred embodiment, the gateway 45 comprises an H.323 gateway and the gatekeeper 55 comprises an H.323 gatekeeper.

The third sub-network of the system 10 is an Operations Support System (OSS) 70. In a presently preferred embodiment, the Operations Support System 70 is comprised of a Subscriber Management Platform (SMP) 75 and a Network Management System (NMS) 80.

The computing devices 20, e.g., PCs, of the system 10 are a component, or network node, of the end user, i.e., subscriber, equipment accessing the wireless access network. In a presently preferred embodiment, a computing device 20 supports a variety of services including, but not limited to, packet data, facsimile and IP packet voice services.

To the core packet data network, a terminal 21 appears as an Internet Protocol (IP) destination node. Thus, a terminal 21 has an associated IP address, and supports processing of the termination of the Internet Protocol for data message transmissions within the wireless access network. In a presently preferred embodiment, a terminal's IP address is changed as the terminal 21 is physically transported to different connection locations in the system 10. Thus, a terminal's IP address is dynamically allocated by the system 10, as needed.

To the Internet Protocol (IP) packet voice network, an H.323 terminal 17 appears as an Internet Protocol (IP) destination node. Thus, an H.323 terminal 17 has an associated IP address, and supports processing of the termination of the

Internet Protocol for voice message transmissions within the wireless access network. In a presently preferred embodiment, an H.323 terminal's IP address is changed as the H.323 terminal 17, or at least the terminal 17 portion of the H.323 terminal 17, i.e., the respective PC and WM 25 of the H.323 terminal 17, is physically transported to different connection locations in the system 10. Thus, an H.323 terminal's IP address is dynamically allocated by the system 10, as needed.

In a presently preferred embodiment, to the IP packet voice network, an H.323 terminal 17 acts as a network endpoint. Thus, to support IP packet voice network processing, an H.323 terminal 17 supports the elements necessary for H.323 communication. These elements include, but are not limited to, an H.323 software protocol stack, for communications processing, vocoding functionality, and audio/video equipment functionality. In a presently preferred embodiment, the vocoding functionality is based on the G.7xx series of recommendations referenced in the H.323 protocol standards. In a presently preferred embodiment, the H.323 protocol functionality runs as an application over the core packet data network applications.

A wireless modem (WM) 25 interfaces with a respective computing device 20 and provides the bridging functionality to enable the computing device 20 to connect to the wireless access system. In a presently preferred embodiment, a WM 25 is connected to a respective computing device 20 via standard wireline cabling 22.

For a packet data transfer, or message transmission, a WM 25 manages the interworking between the respective computing device 20 – WM 25 wireline interface 22. The WM 25 also manages the respective computing device 20 end of the over-the-air interface 27 with a base transceiver station 30, also referred to as a base station. For a packet data transfer, the WM 25 also provides the processing for managing the end point signaling for functions including, but not limited to, authentication, encryption setup, address resolution and dynamic IP address allocation.

In a presently preferred embodiment, on the computing device 20 side, the respective WM 25 supports a PCMCIA (Personal Computer Memory Card International Association) based physical interface, with an extended asynchronous transfer (AT) command set for the respective computing device's control of the WM 25. In one respect, a computing device 20 and a respective WM 25, i.e., a terminal 21 represents a transportable terminal end unit of the system 10 to a base transceiver station, or base station, 30 and the external data networks supported by the system 10. Also, in the same respect, a computing

device 20 and a respective WM 25 of an H.323 terminal 17 represents a transportable terminal end unit of the system 10 to a base transceiver station, or base station, 30, and the external switched circuit networks supported by the system 10.

In a presently preferred embodiment, on the bearer plane, i.e., voice and data message transmission protocol planes, a WM 25 is used as a link layer bridge between a base station 30 and a computing device 20. In a presently preferred embodiment, a WM 25 is not required to support IP address or routing functionality as the respective terminal 21, or H.323 terminal 17, owns the assigned IP address.

A base transceiver station (BTS) 30, or base station, is an integral part of the over-the-air functionality of the system 10. A base station 30 comprises the capability to provide radio coverage to a specific geographical area serviced by the system 10. A base station 30, among other functions, provides a WM 25 connectivity to the backbone of the system 10; i.e., to those network nodes, or elements, and respective communications paths that support connectivity to the services of the network, including access to the external packet data and external switched circuit networks supported by the system 10. A base station 30 comprises the equipment, components and software necessary for bi-directional communication with one or more WMs 25. In a presently preferred embodiment, a base station 30 communicates with a WM 25 via an over-the-air, i.e., radio or wireless, interface 27.

In a presently preferred embodiment, the wireless functionality, i.e., over-the-air interface communications, of the system, or network, 10 is based on the GPRS (General Packet Radio Service) and GSM (Global System for Mobile Communication) protocols. In an alternative embodiment, the wireless functionality of the system 10 is based on the GSM/Edge (Global System for Mobile communication/Enhanced Data rates for GSM Evolution) protocols.

Further, system 10 can be used with other communication system, or protocol, platforms, or communication standards, for the respective wireless, i.e., radio, or over-the-air, communications including, but not limited to, IS-95, Global System for Mobile communication (GSM), Digital AMPS (DAMPS), DECT, Wideband Code Division Multiple Access (WB-CDMA), Wideband Time Division Multiple Access (WB-TDMA), PHS, IS-661, Personal Communications System (PCS), PACS, and all their derivatives.

In a presently preferred embodiment, a base station 30 supports multiple WMs 25. Cell engineering is used to ensure that the number of base stations 30

deployed in a geographic area serviced by the system 10 is sufficient to provide connectivity for the respective computing devices 20 and associated WMs 25, i.e., terminals 21, or for the respective telephones 15 and their associated computing devices 20 and WMs 25, i.e., H.323 terminals 17, connecting to the system 10 from the base station's respective geographical support area.

A base station 30 further supports signaling termination and interworking functionality, including, but not limited to, authentication, encryption setup, address resolution and temporary link layer identity (TLLI), or addressing, allocation, for subsequent voice or packet data message transmissions.

On the network side, a base station 30 interacts via an access router 35 and an IP network 40, for example, but not limited to, e.g., a private IP network, to provide connectivity into one or more external data networks, including the Internet 65, and into one or more external switched circuit networks 50. A base station 30 provides the bridging functionality to relay packet bearer traffic, voice or data, between a WM 25 and the base station 30 and between the base station 30 and respective upstream network interfaces, e.g., the Internet 65 and one or more external switched circuit networks 50.

In a presently preferred embodiment a base station 30 uses an external IP address and supports an IP layer protocol stack functionality for packet data and voice services and subscriber management functions.

An access router 35 provides the base stations 30 of the system 10 connectivity to the external world, e.g., one or more external data networks, including the Internet 65, and one or more external switched circuit networks 50, via an IP network 40. In a presently preferred embodiment, an access router 35 is an off-the-shelf router that supports IP routing and firewalling functionality. In a presently preferred embodiment, a base station 30 communicates with one or more access routers 35 via a wireline interface 32.

An access router 35 further provides termination of network side functionality for mobility management in the system, or network, 10. In a presently preferred embodiment, the Reverse Address Resolution Protocol (RARP) is used in the system 10 to support the transportability feature of a terminal 21 or an H.323 terminal 17. In an alternative embodiment, the Mobile Internet Protocol (IP) is used in the system 10 to support the transportability feature of a terminal 21 or an H.323 terminal 17. In yet another alternative embodiment, the General Packet Radio Service (GPRS) protocol is used in the system 10 to support the transportability feature of a terminal 21 of an H.323 terminal 17.

As previously discussed, in a presently preferred embodiment, the IP network 40 comprises a private IP network 40. The private IP network 40 is a managed IP network, wherein resource management and Quality of Service aspects of the system 10 services are controlled. Connected to the private IP network 40 are the network management elements, or nodes, of the system 10, and one or more access routers 35. In a presently preferred embodiment, the network managed elements, or nodes, include, but are not limited to, an Internet gateway 60, a switched circuit, i.e., voice, gateway 45 and a switched circuit, i.e., voice, gatekeeper 55. In a presently preferred embodiment, the voice gateway 45 comprises an H.323 gateway and the voice gatekeeper 55 comprises an H.323 gatekeeper.

In a presently preferred embodiment, the private IP network 40 communicates with an access router 35 via a wireline interface 37. In a presently preferred embodiment, the private IP network 40 communicates with the Operations Support System 70, and, more specifically, the Subscriber Management Platform (SMP) 75 and the Network Management System (NMS) 80, via respective wireline interfaces 36.

In a presently preferred embodiment, the private IP network 40 provides connectivity for various network managed elements, for example, but not limited to, e.g., the Internet gateway 60, the H.323 gateway 45 and the H.323 gatekeeper 55, via respective wireline interfaces 43.

The Internet gateway 60 provides connectivity to the Internet 65; the private IP network 40 connects to the Internet gateway 60, thereby providing end users, i.e., subscribers, of the system 10 access to the Internet 65. In a presently preferred embodiment, the Internet gateway 60 is an off-the-shelf network element that supports IP routing and firewalling functionality.

In a presently preferred embodiment, the system 10 uses the architecture specified in the H.323 protocol standards for provisioning IP packet voice services. Within the wireless access network, IP packet voice messages are transmitted between two end points, as shown in Figure 3. One endpoint 825 is generally an H.323 terminal 822. The other endpoint 825 is either another H.323 terminal 822 or a switched circuit network 824 supported by the wireless access network. The switched circuit network 824 routes the respective switched transmission format voice messages created from the IP packet voice messages to the appropriate non-network destination.

Referring again to Figure 2, an H.323 gateway 45 is a key element in the IP voice services supported by the system 10. An H.323 gateway 45 provides the

interworking functionality between the H.323 and the switched circuit network transmission and signaling formats.

On the end user, i.e., subscriber, side, an H.323 gateway 45 resides as a peer entity to an H.323 terminal 17. Voice bearer packets and signaling are transferred over the system 10 between an H.323 terminal 17 and an H.323 gateway 45.

On the network side, an H.323 gateway 45 communicates with a switched circuit network 50. In a presently preferred embodiment, an H.323 gateway 45 communicates with a switched circuit network 50 via a wireline interface 47.

In a voice bearer transmission plane, an H.323 gateway 45 provides the interworking functionality between the transmission formats on the user, e.g., H.323 terminal 17, side and the switched circuit network 50 side. On the user side, an H.323 gateway 45 implements vocoded transmission formats used by an H.323 terminal 17. In a presently preferred embodiment, the vocoded transmission formats are based on the G.7xx series of recommendations.

On the switched circuit network 50 side, an H.323 gateway 45 supports the functionality for handling the switched transmission formats of a switched circuit network 50.

An H.323 gateway 45 implements the transcoding function between the vocoded transmission formats of a respective H.323 terminal 17 and the switched transmission formats of a respective switched circuit network 50. Supporting this functionality, an H.323 gateway 45 appears as another H.323 terminal 17 to an H.323 terminal 17. An H.323 gateway 45 translates, in a transparent fashion, the vocoded transmission format voice messages from an H.323 terminal 17 into switched circuit network format voice messages, for transmission to a switched circuit network 50. In the alternate direction, an H.323 gateway 45 translates, also in a transparent fashion, switched circuit network format voice messages from a switched circuit network 50 into respective vocoded transmission format voice messages, for transmission to an H.323 terminal 17.

In a voice signaling plane, an H.323 gateway 45 provides the interworking functionality between the H.323 call signaling and the signaling towards the switched circuit network 50. Supporting this functionality, an H.323 gateway 45 appears as another H.323 terminal 17 to an H.323 terminal 17. An H.323 gateway 45 translates, in a transparent fashion, H.323 call control and capabilities exchange signals from an H.323 terminal 17 into switched circuit network call control and capabilities exchange signals, for transmission to a switched circuit network 50. In the alternate direction, an H.323 gateway 45 translates, also in a

transparent fashion, switched circuit network call control and capabilities exchange signals from a switched circuit network 50 into H.323 call control and capabilities exchanges signals, for transmission to an H.323 terminal 17.

In a presently preferred embodiment, an H.323 gateway 45 is an off-the-shelf element, purchased from a standard H.323 Gateway/Gatekeeper vendor.

In a presently preferred embodiment, an H.323 gatekeeper 55 is another key element in the IP packet voice services supported by the system 10. An H.323 gatekeeper 55 is a logically separate element from an H.323 gateway 45; however, the physical implementation of an H.323 gatekeeper 55 may coexist with an H.323 gateway 45.

Referring again to Figure 3, each endpoint 825 of an IP packet voice message transmission communicates on the wireless access network via an H.323 gatekeeper 820. A Registration and Admissions and Status (RAS) channel is opened, or established, between each endpoint 825 and a respective H.323 gatekeeper 820, prior to the establishment of any other channels between the endpoints 825 and a respective H.323 gatekeeper, or H.323 gatekeepers, 820.

The wireless access network supports a Discovery procedure 830 between an H.323 gatekeeper 820 and one or more endpoints 825 in the wireless access network. The Discovery procedure 830 is used to inform potential endpoints 825 of the existence of the H.323 gatekeeper 820 for voice transmissions. In a presently preferred embodiment, a manual Discovery procedure is used, whereby an H.323 gatekeeper 820 broadcasts its transport, i.e., IP, address to a geographic location, or zone or cell. In an alternative embodiment, an automatic Discovery procedure is used, whereby respective endpoints 825 each initiate protocol transmissions to discover an H.323 gatekeeper 820 they can respectively become associated with.

Once an H.323 gatekeeper 820 is discovered by an endpoint 825, the endpoint 825 executes a Registration procedure 832 with the H.323 gatekeeper 820. Using the Registration procedure 832, an endpoint 825 joins a zone, or cell, managed by a respective H.323 gatekeeper 820, and informs the H.323 gatekeeper 820 of its relevant addresses, i.e., its standard telephone number or E.164 address, and its Internet Protocol (IP) address. The Registration procedure 832 is executed between an H.323 endpoint 825 and an H.323 gatekeeper 820 before any IP packet voice transmissions between the respective endpoint 825 and gatekeeper 820 may commence. Registration establishes a Registration and Admissions and Status (RAS) channel between the endpoint 825 and the H.323 gatekeeper 820.

Referring again to Figure 2, among other functions, an H.323 gatekeeper 55 performs alias address, e.g., standard telephone number or E.164 address, to transport, i.e., IP, address translation. This translation provides a mapping between a telephone number, or E.164 address, and the current IP address of an H.323 terminal 17. An H.323 gatekeeper 55 also dynamically updates the respective mapping of telephone numbers to IP addresses, for H.323 terminals 17 it is associated with, or otherwise communicates with, to reflect the current physical location of an H.323 terminal 17 that has been relocated, i.e., transported, within the system 10.

Referring back to Figure 3, once an endpoint 825 registers with a respective H.323 gatekeeper 820, it periodically executes a Re-Registration procedure 834 with the H.323 gatekeeper 820. Once an endpoint 825 registers with a respective H.323 gatekeeper 820, the H.323 gatekeeper 820 may use the respective RAS channel established between them for executing a Bandwidth Management procedure 838. The Bandwidth Management procedure 838 establishes the bandwidth that an endpoint 825 may use for its respective packet voice message transmissions.

Once an endpoint 825 registers with a respective H.323 gatekeeper 820, the H.323 gatekeeper 820 may use the respective RAS channel established between them for executing a Status procedure 840 with the endpoint 825. The Status procedure 840 provides the H.323 gatekeeper 820 status on the various endpoints 825 registered with it.

Also after registration, an endpoint 825 may execute a De-Registration procedure 842 with the respective H.323 gatekeeper 820. The De-Registration procedure 842 provides the endpoint 825 a mechanism for disassociating itself with the respective H.323 gatekeeper 820.

Further, after registration, an H.323 gatekeeper 820 and a respective endpoint 825 may execute a Call Signaling procedure 836. The Call Signaling procedure 836 establishes a call signaling channel between the endpoint 825 and the H.323 gatekeeper 820, for maintenance of subsequent IP packet voice transmissions, i.e., an IP telephone call, between them. In a presently preferred embodiment, the Call Signaling procedure 836 uses the H.225.0 protocol for establishing a call signaling channel between an H.323 gatekeeper 820 and an endpoint 825. The established call signaling channel is maintained for the duration of the IP telephone call. In a presently preferred mbodiment, the symmetrical signaling method of Annex D/Q.931 is used for the call signaling

procedures; i.e., Q.931 protocol messages are used by the Call Signaling procedure 836.

The initial call signaling message, i.e., an initial admission message, is transmitted between an endpoint 825 and an H.323 gatekeeper 820 via their previously established RAS channel. In a presently preferred embodiment, all subsequent call signaling messages are transmitted via the established call signaling channel.

If the IP packet voice messages, i.e., the IP telephone call, is between two H.323 terminal endpoints 822, the respective H.323 gatekeeper, or H.323 gatekeepers, 820 routes applicable Q.931 protocol messages between the calling and called H.323 terminals 822. If the IP telephone call is between an H.323 terminal 822 and a switched circuit network 824, the respective H.323 gatekeeper, or H.323 gatekeepers, 820 routes the switched circuit format messages generated from Q.931 protocol messages of the H.323 terminal 822 to the switched circuit network 824, and, in the alternative direction, routes Q.931 protocol messages generated from the switched circuit format messages of the switched circuit network 824 to the H.323 terminal 822.

An H.323 gatekeeper 820 may determine to complete a call signaling protocol with the calling/called endpoints 825. In the case of an H.323 terminal 822 to switched circuit network 824 IP telephone call, if the respective H.323 gatekeeper, or H.323 gatekeepers, 820 processes the H.323 call signaling, it thereby directs the H.323 call signaling towards a respective H.323 gateway. The H.323 gateway then provides the process functionality for interworking the H.323 signaling to a switched circuit network signaling format.

An H.323 gatekeeper 820 may alternatively direct the calling/called endpoints 825 to connect the call signaling via each other, without requiring the services of an H.323 gateway.

Too, an H.323 gatekeeper 820 supports Call Control procedures 844, for IP packet voice call control. As shown in Figure 4, the Call Control procedures 844 comprise a variety of procedures including, but not limited to, a Master/Slave Determination procedure 852, a Capability Exchange procedure 854, a Logical Channel Signaling procedure 856, a Mode Request procedure 858, a Round Trip Delay Determination procedure 860 and a Maintenance Loop Signaling procedure 862.

The Master/Slave Determination procedure 852 comprises functionality to resolve conflicts between two H.323 endpoints 825 that are attempting to open a bi-directional channel. Thus, the Master/Slave Determination procedure 852

determines which H.323 endpoint 825 is to act as the master of the IP packet voice channel and which is to act as the slave, for subsequent call control purposes.

The Capability Exchange procedure 854 comprises functionality to support H.323 terminals 822 statusing, or otherwise reporting, their receive and transmit capabilities, and their ability to operate in various mode combinations simultaneously, to a respective H.323 gatekeeper 820. In a presently preferred embodiment, a fixed vocoder type operational mode and receive and transmit capabilities are the default capabilities of a respective H.323 terminal 822. In an alternative embodiment, H.323 terminals 822 are required to report their operational mode, or modes, and their receive and transmit capabilities to an H.323 gatekeeper 820, and no default is assumed.

The Logical Channel Signaling procedure 856 comprises functionality for the opening, i.e., establishment, and closing, i.e., de-allocation, of logical channels for IP packet voice transmissions. In a presently preferred embodiment, unidirectional logical channels are opened, or established or allocated, for respective IP packet voice message transmissions, and thus, asymmetrical operation is supported, whereby the number and type of message streams can be different in the two, i.e., calling and called, directions.

The Mode Request procedure 858 comprises the functionality for an H.323 terminal 822 to indicate its preference for the other H.323 terminal's, i.e., the other H.323 terminal 822 involved in the respective IP telephone call, transmit mode. H.323 terminals 822 acquiesce to preferred transmit mode requests if they are capable of doing so.

The Mode Request procedure 858 also comprises the functionality for an H.323 terminal 822 to indicate its preference for a respective H.323 gatekeeper's transmit mode. Further, an H.323 gatekeeper 820 can use the Mode Request procedure 858 to indicate its preference for a respective H.323 terminal's transmit mode. The requested entity, i.e., an H.323 terminal 822 or an H.323 gatekeeper 820, acquiesces to the preferred transmit mode requests if they are capable of doing so.

The Round Trip Delay Determination procedure 860 comprises functionality for determining the round trip delay between a transmit and a receive H.323 terminal 822 involved in an IP telephone call. The Round Trip Delay Determination procedure 860 also comprises functionality for determining the round trip delay between an H.323 terminal 822 and an H.323 gatekeeper 820 involved in an IP telephone call.

The Maintenance Loop Signaling procedure 862 comprises functionality for establishing maintenance transmission loops, to verify IP packet voice transmission channels in the network.

In a presently preferred embodiment, an H.323 gatekeeper 820 comprises an off-the-shelf element, purchased from a standard H.323 Gateway/Gatekeeper vendor.

Referring to Figure 2, a switched circuit network 50 is a network through which voice, i.e., telephony, calls can be routed. A switched circuit network 50 may comprise, but is not limited to, a public switched telephone network (PSTN) or an integrated services digital network (ISDN).

In a presently preferred embodiment, a network 10 can comprise, or further comprise, one or more Customer Radio Premises Units (CPRUs), as shown in Figure 2A. A CPRU 23 is generally associated with a home or business premise. A CPRU 23 interfaces with one or more computing devices 20, for example, but not limited to, e.g., a personal computer (PC), smart terminal, or a work station, located in or about the respective premise. In a presently preferred embodiment, the CPRU 23 communicates with the respective premise's computing devices 20 via a wireline interface 24. In a presently preferred embodiment, a computing device 20 and a CPRU 23 comprise a terminal 31. A terminal 31 is equivalent to a terminal 21 in the network 10, except that the terminal 31 is generally considered a fixed terminal and the terminal 21 is generally considered a mobile, or transportable, terminal.

A CPRU 23 may further be connected to one or more voice access devices, for example, but not limited to, e.g., a telephone 15, located in or about the respective premise. In a presently preferred embodiment, the CPRU 23 communicates with the respective premise's voice access devices via a wireline interface 24. In a presently preferred embodiment, a voice access device and a CPRU 23 comprise a terminal 33. A terminal 33 is equivalent to a terminal 17 in the network 10, except that the terminal 33 is generally considered a fixed terminal and the terminal 17 is generally considered a mobile, or transportable, terminal.

A CPRU 23 communicates with a base transceiver station 30, also referred to as a base station, supporting the cell, or geographic location the CPRU 23 is located in on a wireless, i.e., over-the-air, or radio, 27 interface. A base station 30 comprises the equipment, components and software necessary for bi-directional communication with one or more CPRUs 23.

In a presently preferred embodiment, the base stations 30 and CPRUs 23 of a network 10 status their own hardware resources to the network 10, including, but not limited to, a unique resource description that identifies the respective resource, i.e., the resource type, the version of the particular resource type, and the location of the resource. The hardware resource information of a respective base station 30 or CPRU 23 is provided to the network 10 by the base station 30 or CPRU 23 upon the respective base station's or CPRU's power on or reset. The hardware resource information of a respective base station 30 or CPRU 23 is also provided to the network 10 by the base station 30 or CPRU 23 as part of a respective hardware failure status report.

In a presently preferred embodiment, the base stations 30 and CPRUs 23 of the network 10 status their own software and firmware resources to the network 10, including, but not limited to, a resource type identification and the version of the respective software or firmware executing on the respective base station 30 or CPRU 23. The software/firmware resource information of a respective base station 30 or CPRU 23 is provided to the network 10 by the base station 30 or CPRU 30 upon the respective base station's or CPRU's power on or reset.

In a presently preferred embodiment, at least one version of all software and firmware files required for base station operation is located in non-volatile base station memory of each respective base station 30 of the network 10. Likewise, in a presently preferred embodiment, at least one version of all software and firmware files required for Customer Premises Radio Unit (CPRU) operation is located in non-volatile CPRU memory of each respective CPRU 23 of the network 10. In a presently preferred embodiment, base stations 30 and CPRUs 23 of the network 10 support updating respective individual software or firmware files. Base stations 30 and CPRUs 23 of the network 10 also support complete respective software/firmware version updates.

The software and firmware files of the respective base stations 30 and CPRUs 23 of the network 10 comprise customization parameters that support customization of respective base stations 30 and CPRUs 23.

The base stations 30 and CPRUs 23 of the network 10 generate and maintain hardware/software/firmware status, and provide this status to the network 10. The hardware/software/firmware status of a base station 30 or CPRU 23 in the network 10 comprises the ability of the respective base station 30 or CPRU 23 to support wireless access services.

Self-testing is performed by each base station 30 and CPRU 23 in the network 10 on power on and reset, to verify their respective correct operations. A

self-test for a base station 30 and a self-test for a CPRU 23 each comprise a loop test for verification of their respective over-the-air interface 27.

Each base station 30 and CPRU 23 in the network 10 supports self-supervision functionality to detect failures due to respective equipment, processing, communications, quality of service and environment conditions. The respective self-supervision functionality further supports providing failure information to the network 10, via hardware status failure reports. In a presently preferred embodiment, reported failures include the type of failure, the severity of the failure and the identity of any failing component of the respective base station 30 or CPRU 23. The self-supervision functionality of each base station 30 and CPRU 23 in the network 10 also comprises determining when a previously detected failure has ceased, or otherwise corrected itself.

In a presently preferred embodiment, whenever a base station 30 of the network 10 is operational, it performs a measurement collection functionality. In a presently preferred embodiment, the measurement collection functionality includes, but is not limited to, the uplink radio quality and signal strength on each base station 30 for all used, i.e., busy, over-the-air, channels, the signal strength on idle, i.e., not used, over-the-air channels, the success rate of over-the-air interface procedures and the availability and usage of the base station's over-the-air resources.

The measured, and/or collected values, or results, are reported to the network 10, based on a network configurable reporting period. Any base station 30 of the network 10 may also be requested by the network 10 to cease measurement value reporting. Further, any base station 30 that was previously requested to cease measurement value reporting may be requested by the network 10 to resume measurement value reporting.

The wireless access system, or network, 100, depicted in Figure 5, is an alternative embodiment wireless access system, or network. The wireless access system 100 comprises a wireless router and concentrator (WRC) 90 that sits upstream of a base station 28. A WRC 90 performs the functions of a wireless access router. Among the functions that a WRC 90 supports is concentration of communication links and processing functionality. A WRC 90 also supports subscriber, e.g., end user, management and authentication functionality. Too, on the network side, a WRC 90 supports the termination of over-the-air encryption processing, for bearer, i.e., voice and data, message transmissions.

In a presently preferred embodiment of system 100, the wireless functionality, i.e., over-the-air interface communications, of the system 100 is

based on the GPRS (General Packet Radio Service) and GSM (Global System for Mobile Communication) protocols. In an alternative embodiment, the wireless functionality of the system 100 is based on the GSM/Edge (Global System for Mobile communication/Enhanced Data rates for GSM Evolution) protocols.

Further, system 100 can be used with other communication system, or protocol, platforms, or communication standards, for the respective wireless, i.e., radio, or over-the-air, communications including, but not limited to, IS-95, Global System for Mobile communication (GSM), Digital AMPS (DAMPS), DECT, Wideband Code Division Multiple Access (WB-CDMA), Wideband Time Division Multiple Access (WB-TDMA), PHS, IS-661, Personal Communications System (PCS), PACS, and all their derivatives.

A WRC 90 provides termination of network side functionality for mobility management. In a presently preferred embodiment of system 100, using a WRC 90 in the system 100, the Reverse Address Resolution Protocol (RARP) is used to support the transportability feature of a terminal 21 or an H.323 terminal 17. In an alternative embodiment, the Mobile Internet Protocol (IP) is used in the system 100 to support the transportability feature of a terminal 21 or an H.323 terminal 17. In yet another alternative embodiment, the General Packet Radio Service (GPRS) protocol is used in the system 100 to support the transportability feature of a terminal 21 of an H.323 terminal 17.

In a presently preferred embodiment of system 100, a significant amount of functionality is transferred from a base station 28 to a WRC 90. This enables the respective base stations 28 to be lighter-weight platforms.

In a presently preferred embodiment, as shown in Figure 6, a centralized operations center supports management of a wireless access system, or network, and the various network nodes, or elements, including, but not limited to, base stations, Internet gateways, H.323 gateways and H.323 gatekeepers, and protocol platforms. In a presently preferred embodiment, the network management architecture 150 for a wireless access network is comprised of a network element management layer (NEML) 160, a network management layer (NML) 170 and a service management layer (SML) and business management layer (BML) (collectively 180).

In a presently preferred embodiment, network element management is provided by a mixture of off-the-shelf and customized platforms that function as first level managers of specific domains. In a presently preferred embodiment, the network element management layer 160 is comprised of a gateway management platform 162, for managing the network's gateway domain, i.e., gateway

elements, a router management platform 164, for managing the network's router domain, i.e, router elements, and a wireless access network management platform 166, for managing the network's base station domain, i.e., base station elements.

The gateway management platform 162 provides the functionality for provisioning, administration, statusing and performance monitoring of the gateways of the network. In a presently preferred embodiment, the gateway management platform 162 also provides the functionality for provisioning, administration, statusing and performance monitoring of the gatekeepers of the network. In a presently preferred embodiment, the gateway management platform 162 comprises off-the-shelf management platforms supplied by respective Internet gateway and H.323 gateway and/or H.323 gatekeeper vendors.

The router management platform 164 provides the functionality for provisioning, administration, statusing and performance monitoring of the routers of the network. In a presently preferred embodiment, the router management platform 164 is an off-the-shelf management platform supplied by a router vendor.

The wireless access network management platform 166 is a general purpose management platform for management of the base stations 30 of the wireless access network. In an embodiment, the wireless access network management platform 166 also provides the functionality for managing the base stations 28 and the wireless router and concentrator (WRC) 90 of network, or system, 100.

The network management layer 170 comprises a scalable network node management (NNM) platform 172 for providing centralized network node management. In a presently preferred embodiment, the network node management platform 172 consolidates the diverse management requirements of the various gateways, gatekeepers, routers and base stations of the wireless access network into an integrated management view. The network node management platform 172 provides standard network management functionality, including, but not limited to, configuration, fault and performance management. Additionally, the network node management platform 172 comprises an architecture which incorporates event management, database control and general network node, or element, security features for the respective wireless access network.

In a presently preferred embodiment, the network node management platform 172 provides standard APIs (application platform interfaces) which allow attachment of third party applications to the wireless access network for purposes

including, but not limited to, trouble-shooting and error management, asset management and system, service and functionality analysis.

The service management and business management layers 180 comprise a Subscriber Management Platform (SMP) 182. Referring to Figure 7, the Subscriber Management Platform (SMP) 182 supports various subscriber-orientated functionality, or procedures 190. In a presently preferred embodiment, the SMP 182 supports a Customer Registration procedure 191, a Customer Authentication procedure 192, a Customer Rating procedure 193, a Customer Billing procedure 194 and a Customer Management procedure 195.

The Customer Registration procedure 191 includes, but is not limited to, functionality for the collection, storage and management of customer data for customer provisioning and billing. The customer data includes, but is not limited to, the subscriber profile of the respective customer, which includes, but is not limited to, subscription information on services and other parameters that have been assigned the respective subscriber of the network for an agreed contractual period.

The Customer Authentication procedure 192 provides network protection against fraud. In a presently preferred embodiment, the wireless access network supports both subscriber authentication and terminal authentication functionality. For packet data services, subscriber authentication is generally performed via the wireless access and Internet Protocol (IP) network nodes in an end-to-end, i.e., flow-through, and generally transparent, fashion. For voice services, subscriber authentication is generally performed between an H.323 terminal and a gatekeeper. In a presently preferred embodiment, a challenge/response process and the Challenge Handshake Authentication Protocol (CHAP) are used for subscriber authentication. In an alternative embodiment, a user id/password technique and the Password Authentication Protocol (PAP) are used for subscriber authentication.

Terminal authentication in the wireless access network is used to authenticate a terminal or H.323 terminal with the network. In a presently preferred embodiment, terminal authentication involves three network components: a respective WM 700 of the terminal or H.323 terminal, the base station 704 of the cell, or zone, the WM 700 is located in, and the subscriber management platform (SMP) 708 of the wireless access network, as shown in Figure 8. When using a Customer Premises Radio Unit (CPRU), terminal authentication generally involves the respective CPRU, the base station of the

cell, or zone, the CPRU is located in, and the SMP of the wireless access network.

The WM 700 automatically initiates the terminal authentication process upon power on or when it is moved, or transported, with its respective terminal or H.323 terminal to a new base station cell. In a presently preferred embodiment, the WM 700 communicates with the respective base station 704 for terminal authentication via the Terminal Management Protocol (TMP). The WM 700 has a secret key installed in the factory; the secret key is associated with the WM's unique universal identifier; i.e., the WM's International Mobile Subscriber Identity (IMSI). The WM 700 also comprises dedicated circuitry and/or software to compute responses to given terminal authentication challenges issued by the Subscriber Management Platform (SMP) 708 of the wireless access network, using its secret key.

A base station 704 acts as a relay between the WM 700 and the SMP 708 for terminal authentication purposes. The base station 704 communicates with the WM 700 for terminal authentication purposes via the Terminal Management Protocol (TMP). The secure Logical Link Control (LLC) protocol is the underlying transmission protocol for the TMP, as further discussed with regard to Figure 12.

In a presently preferred embodiment, the base station 704 communicates with the Subscriber Management Platform (SMP) 708 of the wireless access network for terminal authentication purposes via the Remote Authentication Dial In Service (RADIUS) protocol. The unsecure User Datagram Protocol (UDP) is the underlying transmission protocol for the RADIUS protocol, as further discussed with regard to Figure 12.

Upon execution of the terminal authentication protocol between a WM 700 and the network, i.e., the Subscriber Management Platform (SMP) 708, the base station 704 retains the terminal authentication status of the respective WM 700. The base station 704 thereafter uses the WM's terminal authentication status for admitting, or denying, the WM 700 subsequent access to the network. For example, a base station 704 will deny network access to a WM 700 that was not previously properly authenticated via the terminal authentication procedure.

The Subscriber Management Platform (SMP) 708 stores pairs of WM 700 identities and respective secret keys. When an "Access Request" message is received by the SMP 708, via a base station 704, from a WM 700, requesting access to the network, the SMP 708 replies with an "Access Challenge" message. In a presently preferred embodiment, the "Access Challenge" message includes a random number. Upon receiving the "Access Challenge" message from the SMP

708, via a base station 704, the WM 700 responds accordingly. Upon receiving the WM's response, again via a base station 704, the SMP 708 transmits an "Access Accept" message to the WM 700, via the base station 704, if the WM's received response is a correct response to the SMP's "Access Challenge" message. If not, the SMP 708 transmits an "Access Reject" to the WM 700, via the base station 704.

In a presently preferred embodiment, a "Vendor Specific" field supported by the RADIUS protocol is included in the "Access Accept" messages sent between a respective WM 700 and the SMP 708. In a presently preferred embodiment, the "Vendor Specific" field is also included in "Access Request" messages sent from a WM 700 to a base station 704, for requesting access to the services of the network.

The "Vendor Specific" field is used to carry terminal subscription information. In a presently preferred embodiment, the "Vendor Specific" field is used to carry the Quality of Service (QoS) profile subscribed for by the end user, i.e., subscriber, associated with a given WM 700. The QoS profile in the "Access Request" message is used by the receiving base station 704, for policing purposes, for example, but not limited to, denying a WM 700 a service request that is not covered by the WM's QoS.

A CPRU generally operates in the same manner as a WM 700 for terminal authentication. A respective CPRU automatically initiates the terminal authentication process upon power on. In a presently preferred embodiment, a CPRU communicates with a respective base station for terminal authentication via the Terminal Management Protocol (TMP). The CPRU has a secret key installed in the factory; the secret key is associated with the CPRU's unique universal identifier; i.e., the CPRU's International Mobile Subscriber Identity (IMSI). The CPRU also comprises circuitry and/or software to compute responses to give terminal authentication challenges issued by the Subscriber Management Platform (SMP) of the wireless access network, using its secret key.

A base station acts a relay between a CPRU and the SMP for terminal authentication purposes. Further, upon execution of the terminal authentication protocol between a CPRU and the network, i.e., the Subscriber Management Platform (SMP), the respective base station retains the terminal authentication status of the respective CPRU. The base station thereafter uses the CPRU's terminal authentication status for admitting, or denying, the CPRU subsequent access to the network. For example, a base station will deny network access to a

CPRU that was not previously properly authenticated via the terminal authentication procedure.

Referring again to Figure 7, the Customer Rating procedure 193 includes, but is not limited to, the creation and maintenance of flexible pricing plans.

The Customer Billing procedure 194 supports the generation of flexible customer billings. The Customer Billing procedure 194 also supports real time and invoice-based payment requests. The Customer Billing procedure 194 further supports billing customers of the system, or network, e.g., subscribers, in one or more of a multiple number of currencies.

The Customer Management procedure 195 generates and provides network management access to customer, i.e., subscriber, information including, but not limited to, subscription profiles, subscription activity and customer account balances. In a presently preferred embodiment, subscription profiles include, but are not limited to, customer identification, customer service support requests and the Quality of Service (QoS) subscribed for. In a presently preferred embodiment, subscription activity information includes, but is not limited to, respective subscribers' usage, in time, of respective services supported by the network. In a presently preferred embodiment, customer account balances include, but are not limited to, the monetary amount, for example, but not limited to, e.g., dollars, a respective subscriber owes for the services used on the network.

The wireless access network comprises four planes for communication, as shown in Figure 9. A signaling plane 200 includes a packet data signaling plane 205 for communications signaling for packet data transfers, or transmissions. The signaling plane 200 also comprises a voice signaling plane 210 for communications signaling for packet voice transfers, or transmissions.

A bearer plane 220 includes a packet data bearer plane 225 for packet data transmissions. The bearer plane 220 also comprises a voice bearer plane 230 for IP packet voice transmissions.

In a presently preferred embodiment, the packet data signaling plane 205 comprises functions, or procedures 240, for the control, support and maintenance of the packet data bearer plane 225, i.e., packet data transmission plane, functionality, as shown in Figure 10.

The packet data signaling plane procedures 240 comprise a procedure 201 for the initial connection establishment of a terminal, i.e., the establishment of a physical transmission path, or connection, or communication channel, from the wireless modem (WM) of a terminal to the base station of the cell the terminal is located in, for the subsequent receipt and transmission of packet data. The

connection establishment procedure 201 also comprises functionality for the establishment of a physical transmission path, or connection, or communication channel, from the Customer Premises Radio Unit (CPRU) comprising a terminal to the base station of the cell the terminal is located in, for the subsequent receipt and transmission of IP packet data.

The packet data signaling plane procedures 240 also comprise a procedure 207 for the subsequent de-allocation, or release, of an established packet data transmission path.

The packet data signaling plane procedures 240 also comprise a procedure 202 for terminal authentication. Further, the packet data signaling procedures 240 comprise a procedure 203 for the wireless access network's dynamic allocation of internet protocol (IP) addresses to terminals.

The packet data signaling plane procedures 240 also comprise a procedure 204 for the network's assignment of temporary logical link layer addresses, i.e., a temporary logical link identity (TLLI), to the wireless modems (WMs), or CPRUs, of respective terminals, for terminal communication addressing within the wireless access network. A TLLI is a temporary terminal identity that provides subscriber confidentiality; i.e., with the use of TLLIs, the user identity on the over-the-air interface of the wireless access network is protected from disclosure to unauthorized individuals, entities or processes. A purpose of using a TLLI then is to protect the privacy of the identity of the subscribers using the over-the-air resources of the wireless access network.

A TLLI identifies a network terminal. In a presently preferred embodiment, the relationship between the TLLI and the fixed address of a terminal, i.e., the terminal's International Mobile Subscriber Identity (IMSI), is known only to the respective WM of the terminal, or the respective CPRU of the terminal, and the base station of the network that the terminal communicates with. In a presently preferred embodiment, the IMSI of a terminal is used as its wireless access subscriber authentication value and its billing identity.

The IMSI is structured into a Mobile Country Code (MCC) plus (+) a Mobile Network Code (MNC) plus (+) a Mobile Station Identification Number (MSIN). A specific, unique, Mobile Network Code is associated with a wireless access network.

A TLLI is allocated to a terminal at power up and when the terminal relocates to an alternative base station cell in the network. A TLLI is allocated via Terminal Management Protocol (TMP) signaling between the respective WM of the terminal, or CPRU of the terminal, and the base station it is communicating

with. The base station the WM communicates with allocates the specific TLLI to the WM of the terminal. Too, the base station a CPRU communicates with allocates the specific TLLI to the CPRU associated with a respective terminal.

The packet data signaling plane procedures 240 also comprise a procedure 206 for the establishment of an encryption mode for packet data transmissions. In a presently preferred embodiment, the encryption scheme is based on a public key scheme using the RC4 algorithm. The encryption scheme requires a key exchange procedure to be executed as a signaling exchange between a WM of a terminal and the base station of the cell the terminal is located in, upon power on of the WM and when the terminal relocates to an alternative base station cell in the network. Likewise, the encryption scheme requires a key exchange procedure to be executed as a signaling exchange between a CPRU of a terminal and the base station of the cell the terminal is located in, upon power on of the CPRU. The terminal management protocol (TMP) is used to support encryption signaling.

In a presently preferred embodiment, the encryption procedure 206 includes, but is not limited to, enabling and disabling encryption for packet data transmissions on the over-the-air interface between a WM, or CPRU, and a respective base station. The encryption procedure 206 also supports the derivation of keys to be used to encrypt and decrypt messages, if encryption is enabled. In a presently preferred embodiment, if encryption is enabled, the encryption keys are supplied to the respective logical link control (LLC) layers, as further discussed with reference to Figure 17, of the respective WM, or CPRU, and base station protocol stacks.

The packet data bearer, or transmission, plane 225 of Figure 9 is a wireless sub-network, operating underneath the Internet Protocol (IP). In a presently preferred embodiment, the packet data bearer plane 225 comprises a layered protocol structure that supports user information, i.e., packet data transmissions, and associated user information data transmit control procedures. The user information data transmit control procedures include, but are not limited to, packet data transmission flow control, and data transmission error detection, error correction and error recovery.

In a presently preferred embodiment, the voice signaling plane 210 comprises functions, or procedures 245, for the control, support and maintenance of the voice bearer plane 230, i.e., voice transmission plane, as shown in Figure 11.

The voice signaling plane procedures 245 comprise a procedure 211 for the initial connection establishment of an H.323 terminal, i.e., the establishment of

a physical transmission path, or connection, or communication channel, from the wireless modem (WM) of an H.323 terminal to the base station of the cell the H.323 terminal is located in, for the subsequent receipt and transmission of IP packet voice messages. The connection establishment procedure 211 also comprises functionality for the establishment of a physical transmission path, or connection, or communication channel, from the Customer Premises Radio Unit (CPRU) comprising an H.323 terminal to the base station of the cell the H.323 terminal is located in, for the subsequent receipt and transmission of IP packet voice messages.

The voice signaling plane procedures 245 also comprise a procedure 214 for the subsequent de-allocation, or release, of an established IP packet voice transmission channel, or path.

The voice signaling plane procedures 245 also comprise procedures 216 for subscriber and terminal authentication. The voice signaling procedures 245 also comprise a procedure 212 for the wireless access network's dynamic allocation of internet protocol (IP) addresses to H.323 terminals.

The voice signaling plane procedures 245 further comprise a procedure 213 for the network's assignment of temporary logical link layer addresses, i.e., a temporary logical link identity (TLLI), to the wireless modems (WMs), or CPRUs. of respective H.323 terminals, for terminal communication addressing within the wireless access network. A TLLI identifies a network H.323 terminal, e.g., a telephone, a personal computer (PC) and a wireless modem (WM) combination, or a telephone and a Customer Premises Radio Unit (CPRU) combination. In a presently preferred embodiment, the relationship between the TLLI and the fixed address of an H.323 terminal, i.e., the H.323 terminal's International Mobile Subscriber Identity (IMSI), is known only to the respective WM, or CPRU, of the H.323 terminal and the base station of the network that the H.323 terminal communicates with.

A TLLI is allocated to an H.323 terminal at power up and when the H.323 terminal relocates to an alternative base station cell in the network. A TLLI is allocated via Terminal Management Protocol (TMP) signaling between the respective WM , or CPRU, of the H.323 terminal and the base station it is communicating with. The base station the WM, or CPRU, communicates with allocates the specific TLLI to the respective WM or CPRU of the H.323 terminal.

The voice signaling plane procedures 245 also comprise a procedure 217 for the establishment of an encryption mode for packet voice transmissions. In a presently preferred embodiment, the encryption procedure 217 includes, but is not

limited to, enabling and disabling encryption for packet voice transmissions on the over-the-air interface between a WM, or CPRU, and a respective base station.

The voice bearer, or transmission, plane 230 of Figure 9 is a wireless sub-network, operating underneath the Internet Protocol (IP). In a presently preferred embodiment, the voice bearer plane 230 comprises a layered protocol structure that supports user information, i.e., voice transmissions, and associated user information voice transmit control procedures. The user information voice transmit control procedures include, but are not limited to, IP packet voice transmission flow control, and voice transmission error detection, error correction and error recovery.

A presently preferred embodiment of a packet data signaling plane architecture 250, shown in Figure 12, for use with a terminal comprising a wireless modem (WM), comprises a protocol stack 255 for a WM, a protocol stack 270 for a base station, or base transceiver station (BTS), and a protocol stack 290 for a subscriber management platform (SMP) of the respective network management system.

In a presently preferred embodiment, the protocol stack 255 for a wireless modem (WM) comprises a radio physical layer (RF PHL) 256, a radio link control/medium access control (RLC/MAC) layer 259, a logical link control (LLC) layer 260 and a terminal management protocol (TMP) layer 261.

In a presently preferred embodiment, on the wireless modem (WM) side, the protocol stack 270 for a base station comprises a radio physical layer (RF PHL) 271, a radio link control/medium access control (RLC/MAC) layer 284, a logical link control (LLC) layer 274 and a terminal management protocol (TMP) layer 275.

In a presently preferred embodiment, the radio physical layer 256 of the WM protocol stack 255 and the radio physical layer 271 of the base station protocol stack 270 each comprise a GPRS/GSM (General Packet Radio Service/Global System for Mobile communication) radio interface. In an alternative embodiment, the radio physical layer 256 of the WM protocol stack 255 and the radio physical layer 271 of the base station protocol stack 270 each comprise a GSM/Edge (Global System for Mobile communication/Enhanced Data rates for GSM Evolution) radio interface. The respective radio physical layers 256 and 271 each conceptually consist of two sub-layers, defined by their respective functionality.

The first sub-layer, the physical RF sub-layer, performs the modulation of the physical waveform signals for signaling traffic, for subsequent transmission on

the over-the-air interface between a WM and a base station. The modulation is based on the sequence of bits received from the second sub-layer, the physical link sub-layer. The physical RF sub-layer also performs the demodulation of received waveform signals for signaling traffic, into a sequence of bits which are then transferred to the physical link sub-layer for interpretation.

The second sub-layer, the physical link sub-layer, provides the services for the actual signal traffic transmissions over a physical, wireless, channel between a wireless modem (WM) and a base station. The physical link sub-layer functionality involves signaling traffic transmissions and includes, but is not limited to, signaling message transmission, unit framing, data coding and the detection and correction of physical medium transmission errors, for example, but not limited to, e.g., parity errors. The physical link sub-layer utilizes the services of the respective physical RF sub-layer to perform its functions.

The radio link control/medium access control (RLC/MAC) layer 259 of the wireless modem (WM) protocol stack 255 and the RLC/MAC layer 284 of the base station protocol stack 270 are each comprised of a radio link control function, 258 and 273 respectively, and a medium access control function, 257 and 272 respectively. In a presently preferred embodiment, the RLC/MAC layers 259 and 284 of the respective WM protocol stack 250 and base station protocol stack 270 are based on the GPRS/GSM (General Packet Radio Service/Global System for Mobile communication) protocols. In an alternative embodiment, the RLC/MAC layers 259 and 284 of the respective WM protocol stack 250 and base station protocol stack 270 are based on the GSM/Edge (Global System for Mobile communication/Enhanced Data rates for GSM Evolution) protocols.

The respective medium access control (MAC) layers 257 and 272 are responsible for providing data and signal multiplexing on both uplink and downlink channels of the over-the-air interface between a wireless modem (WM) and a base station. The control for the multiplexing function between a base station and a WM resides with the respective base station protocol stack 270.

For WM-originated channel access, the MAC layer 257 of the WM protocol stack 255 also provides contention resolution functionality between channel access attempts. Thus, the MAC layer 257 of a WM protocol stack 255 executes a contention resolution protocol when the WM attempts to obtain a communication channel on a respective base station, for subsequent communication with the base station.

For WM-originated channel access, the MAC layer 272 of the base station protocol stack 270 provides contention resolution functionality between two or more terminals attempting to gain access to the same base station channel(s).

For network-originated channel access, the MAC layer 272 of a base station protocol stack 270 is responsible for scheduling the various terminal access attempts. Thus, the MAC layer 272 of a base station protocol stack 270 coordinates subsequent terminal network access attempts when the network desires to establish a communication channel with a terminal.

The MAC layer 272 of a base station protocol stack 270 also comprises functionality for the priority management and handling of bearer packet data traffic, i.e., packet data message transmissions.

The radio link control (RLC) layers 258 and 273 of the respective wireless modem (WM) protocol stack 255 and the base station protocol stack 270 provide a radio-dependent reliable link on a wireless modem/base station over-the-air transmission interface. The RLC layer 258 of a WM protocol stack 250 is responsible for the transfer, or transmission, of logical link control (LLC) frames of information, i.e., packet data signaling messages, on the over-the-air interface between the respective WM and a base station. The RLC layer 258 is also responsible for the segmentation of LLC frames into one or more radio link control (RLC) blocks, for physical transmission on the over-the-air interface to a respective base station. The RLC layer 258 also provides the functionality for re-assembly of RLC blocks received on the over-the-air interface, from a base station, into respective LLC frames.

The RLC layer 273 of a base station protocol stack 270 is responsible for the transfer, or transmission, of logical link control (LLC) frames of information, i.e., packet data signaling messages, on the over-the-air interface between the respective base station and the wireless modem (WM) of a terminal. The RLC layer 273 is also responsible for the segmentation of LLC frames into one or more radio link control (RLC) blocks, for physical transmission on the over-the-air interface to a respective WM. The RLC layer 273 also provides the functionality for re-assembly of RLC blocks received on the over-the-air interface, from the WM of a terminal, into respective LLC frames.

The RLC layer 258 of a wireless modem (WM) protocol stack 255 and the RLC layer 273 of a base station protocol stack 270 are responsible for maintaining and executing backward error correction procedures that enable selective retransmission of uncorrectable radio link control (RLC) blocks transmitted between a base station and the WM of a terminal on the over-the-air interface.

The RLC/MAC layer 284 of a base station protocol stack 270 supports the execution of algorithms for radio resource management functions, including, but not limited to, communications resource, i.e., over-the-air channel, management and resource, i.e., over-the-air channel, scheduling.

The logical link control (LLC) layer 260 of a wireless modem (WM) protocol stack 255 provides a reliable, radio-independent, logical link for communications between the respective WM and a base station. Likewise, the logical link control (LLC) layer 274 of a base station protocol stack 270 provides a reliable, radio-independent, logical link for communications between the respective base station and a WM. Logical Link Control (LLC) links are used to transfer packet data signaling traffic between a WM and a base station in the packet data signaling plane. Thus, an LLC link is first established between a WM and a base station, for subsequent packet data signaling transmissions between them. If a terminal is moved to a new base station cell, the respective WM establishes a new LLC link with the base station of the new cell, prior to any subsequent signaling transmissions between them.

In a presently preferred embodiment, the LLC protocol employed in the logical link control (LLC) layers 260 and 274 of a WM protocol stack 255 and a base station protocol stack 270 respectively is specified in the GPRS (General Packet Radio Service) Specification 04.64. This LLC protocol is designed to be independent of the underlying radio protocols for over-the-air interface transmissions. A temporary logical link identity (TLLI) assigned to a terminal is used for addressing at the LLC layers 260 and 274.

The terminal management protocol (TMP) layer 261 of a wireless modem (WM) protocol stack 255 and the TMP layer 275 of a base station protocol stack 270 each provides peer-to-peer procedures between the respective WM and base station, to support network terminal management procedures. The TMP layers 261 and 275 of a respective WM protocol stack 255 and a respective base station protocol stack 270 support a variety of procedures, or functions, 740, as shown in Figure 13.

The respective TMP layers 261 and 275 support procedures for terminal authentication 742. Generally, the terminal authentication procedures 742 prevent the unauthorized use of the respective wireless access network. The terminal authentication procedures 742 also are used to prevent fraudulent impersonations of valid end users, or subscribers, on the network. A presently preferred terminal authentication procedure 742 is previously described, with reference to Figure 8.

The TMP layers 261 and 275 of a respective WM protocol stack 255 and a respective base station protocol stack 270 also support the establishment, or setup, 744 of encryption functionality for subsequent bearer packet data traffic transmissions. The respective TMP layers 261 and 275 support key exchange signaling transmissions between the WM and the base station, for encryption and decryption of bearer packet data traffic transmissions between them. The encryption establishment functionality 744 terminates on the base station that the WM communicates with, and, therefore, requires no interworking within the base station for further upstream network management or control.

The respective TMP layers 261 and 275 also comprise a procedure 746 for the signaling transmissions required for the allocation of a temporary logical link identity (TLLI) to the wireless modem (WM) of a respective terminal, for terminal communication addressing purposes. A TLLI is used for addressing a terminal at the LLC layer 260 of a WM protocol stack 255 and the LLC layer 274 of a base station protocol stack 270. The assigned TLLI is provided to the respective LLC layers 260 and 274 by the respective TMP layers 261 and 275. The TLLI allocation signaling is between a WM and a base station, and the TLLI is allocated to the WM by the base station.

The TMP layer 261 of a WM protocol stack 255 and the TMP layer 275 of a base station protocol stack 270 also each support the respective signaling transmissions required for the network's dynamic allocation of IP (Internet Protocol) addresses 748 to the wireless modems (WMs) of associated terminals. Dynamic IP address allocation supports transportability of terminals within the wireless access network.

In a presently preferred embodiment, the over-the-air address resolution signaling for dynamic IP address allocation is based upon the Reverse Address Resolution Protocol (RARP). On the network side, the base station that the respective WM communicates with interworks the over-the-air address resolution signaling into RARP signaling, for transmission to a respective access router. This network signaling for dynamic IP address allocation establishes a bridge through a base station for the subsequent transport, or transmission, of packet data and voice, and signaling messages, between the respective WM and an access router of the wireless access network.

In a presently preferred embodiment, a base station supplies the interworking functionality between a wireless modem (WM) of a terminal and the Subscriber Management Platform (SMP) of the respective Network Management System (NMS). In a presently preferred embodiment, the protocol stack 270 for a

base station's interworking with the Subscriber Management Platform (SMP) comprises a T1 interface layer 276, a frame relay layer 277, an Internet protocol (IP) layer 278, a user datagram protocol (UDP) layer 279 and a RADIUS client layer 280. In a presently preferred embodiment, the protocol stack 290 for the SMP comprises an IP layer 283, a UDP layer 282 and a RADIUS server layer 281.

RADIUS is an Internet Protocol (IP) based protocol used for carrying authentication and configuration information between a client entity, i.e., a subscriber terminal and a shared authentication server on the network. In a presently preferred embodiment, a base station acts as the proxy RADIUS client on behalf of all the wireless modems (WMs) located in the cell it services, and executes the RADIUS protocol with the Subscriber Management Platform (SMP) of the respective Network Management System (NMS) of the network. The SMP, for its part, acts as the RADIUS server.

The RADIUS protocol and the RADIUS client layer 280 of the base station protocol stack 270 are used to transmit and receive signaling information, or packets or messages, for the terminal authentication procedure, for the subscriber terminals of the network. The RADIUS protocol and the RADIUS server layer 281 of the SMP protocol stack 290 are likewise used to transmit and receive signaling information for the terminal authentication procedure.

A base station interworks the over-the-air terminal authentication protocols between the respective base station and the wireless modems (WMs) of the terminals in its cell, with the RADIUS client-server protocols executed between the base station and the Subscriber Management Platform (SMP) acting as the RADIUS server of the network. In a presently preferred embodiment, the network uses the MD5 authentication algorithm. The two endpoints, or network nodes, in the wireless access system that execute the MD5 authentication algorithm are a WM and the SMP acting as the RADIUS server of the network.

The RADIUS protocol and the RADIUS server layer 281 of the SMP protocol stack 290 and the RADIUS client layer 280 of the base station protocol stack 270 also support the Subscriber Management Platform (SMP) transmitting and receiving subscriber profile information to and from a base station.

As previously noted, in a presently preferred embodiment, the protocol stack 270 for a base station's interworking with a Subscriber Management Platform (SMP) of the respective Network Management System (NMS) comprises a T1 interface layer 276, a frame relay layer 277, an Internet Protocol (IP) layer 278, a User Datagram Protocol (UDP) layer 279 and a RADIUS client layer 280.

Also, as previously noted, the protocol stack 290 for a Subscriber Management Platform (SMP) comprises an IP layer 283, a UDP layer 282 and a RADIUS server layer 281.

In a presently preferred embodiment, the User Data Protocol (UDP) layer 279 of the base station protocol stack 270 and the UDP layer 282 of the SMP protocol stack 290 each provide the primary mechanism for the respective network entities to transmit and receive unsecure datagrams, i.e., unsecure signaling messages, to and from their peer entities in the network. In the packet data signaling plane, the respective UDP layers 279 and 282 are used to transport RADIUS protocols between a base station and the Subscriber Management Platform (SMP) of the wireless access network.

The Internet Protocol (IP) layer 278 of a base station protocol stack 270 and the IP layer 283 of the Subscriber Management Platform (SMP) protocol stack 290 support the connectionless network transmission layer protocol for routing RADIUS protocol signaling messages between the SMP and the base stations of the network. In a presently preferred embodiment, the respective IP layers 278 and 283 use IP version 4. In an alternative embodiment, the respective IP layers 278 and 283 use IP version 6.

In a presently preferred embodiment, the IP layer 278 of the base station protocol stack 270 fulfills the requirements specified in RFC 1490, which is the standard for running IP messages over frame relay transmission channels.

In a presently preferred embodiment, the frame relay layer 277 of a base station protocol stack 270 provides the link layer transport protocol between the respective base station and the system, via an access router, not shown. Generally, frame relay is used for the transport, i.e., transmission, of both signaling information and bearer traffic, e.g., voice and data information, or messages. In the packet data signaling plane specifically, the frame relay layer 277 of the base station protocol stack 270 is used to transmit signaling information, or messages, between the respective base station and the Subscriber Management Platform (SMP) of the network, via an access router.

In a presently preferred embodiment, for signaling information transmissions, permanent virtual circuits (PVCs) are used per respective base station, and the frame relay protocols run under the Internet Protocol (IP).

The T1 interface layer 276 of the base station protocol stack 270 comprises the protocols and procedures for managing a physical T1 communication interface between the respective base station and an access router (not shown). The T1 communication interface is a standard wireline interface. In the packet data

signaling plane specifically, the T1 interface layer 276 of the base station protocol stack 270 is used to transmit signaling information, or messages, between the respective base station and the Subscriber Management Platform (SMP) of the network, via an access router.

A presently preferred embodiment of a packet data bearer plane architecture 370, shown in Figure 14, for use with a terminal comprising a wireless modem (WM), comprises a protocol stack 300 for a personal computer (PC) of a terminal, a protocol stack 320 for a wireless modem (WM) of a terminal, a protocol stack 340 for a base station (or base transceiver station (BTS)), and a protocol stack 360 for an access router.

In a presently preferred embodiment, the protocol stack 300 for a PC comprises a physical link layer 302, a modem command layer 304, an Internet Protocol (IP) layer 306 and an applications layer 308. In a presently preferred embodiment, on the PC-side the protocol stack 320 for a respective wireless modem (WM) comprises a physical link layer 321 and a modem command layer 322. In a presently preferred embodiment, a WM acts as a bridge entity between a respective PC and a base station.

The PC physical link layer 302 and the WM physical link layer 321 each comprise the functionality for managing the physical wireline interface between the respective PC and the respective wireless modem (WM), which together comprise a network subscriber terminal. In an embodiment, the PC physical link layer 302 and the WM physical link layer 321 each support the Personal Computer Memory Card International Association (PCMCIA) protocol.

The PC modem command layer 304 and the WM modem command layer 322 each comprise modem command functionality for commanding and statusing, between the respective PC and the respective wireless modem (WM), the modem of the WM. In a presently preferred embodiment, the respective modem command layers 304 and 322 comprise an extended asynchronous transmission (AT) command set, or protocol, based on the Global System for Mobile communication (GSM) standard.

The Internet Protocol (IP) layer 306 of the PC protocol stack 300 in the packet data bearer plane supports the network IP for transmitting packet data messages between the terminal the respective PC is a part of, and an access router in the network.

The applications layer 308 of the PC protocol stack 300 supports the application functionality for packet data transmissions, including, but not limited to, transmission flow control and error detection, error correction and rror recovery.

In a presently preferred embodiment, on the base station side, a wireless modem (WM) protocol stack 320 comprises a radio physical layer (RF PHL) 323, a radio link control/medium access control (RLC/MAC) layer 324, a logical link control (LLC) layer 325 and a Subnetwork Dependent Convergence Protocol (SNDCP) layer 326. In a presently preferred embodiment, on the WM side, a base station protocol stack 340 comprises an RF PHL layer 341, an RLC/MAC layer 348, an LLC layer 344 and an SNDCP layer 345

The respective RF PHL layers 323 and 341 of the WM protocol stack 320 and the base station protocol stack 340 are equivalent to the respective RF PHL layers 256 and 271 of the WM protocol stack 255 and the base station protocol stack 270 of Figure 12, except the RF PHL layers 323 and 341 support packet data, rather than signaling, traffic transmissions. The respective RLC/MAC layers 324 and 348 of the WM protocol stack 320 and the base station protocol stack 340 are equivalent to the respective RLC/MAC layers 259 and 284 of the WM protocol stack 255 and the base station protocol stack 270 of Figure 12, except the RLC/MAC layers 324 and 348 support packet data, rather than signaling, traffic transmissions. The respective LLC layers 325 and 344 of the WM protocol stack 320 and the base station protocol stack 340 are equivalent to the respective LLC layers 260 and 274 of the WM protocol stack 255 and the base station protocol stack 270 of Figure 12, except the LLC layers 325 and 344 support packet data, rather than signaling, traffic transmissions.

In a presently preferred embodiment, the Subnetwork Dependent Convergence Protocol (SNDCP) layer 326 of the wireless modem (WM) protocol stack 320 and the SNDCP layer 345 of the base station protocol stack 340 each comprise part of the wireless middleware entity functionality of the network that plugs, or otherwise connects or overlaps, the network functionality onto the physical radio components of the network. The Subnetwork Dependent Convergence Protocol (SNDCP) is executed between a WM and a base station. The SNDCP layer 326 of the WM protocol stack 320 and the SNDCP layer 345 of the base station protocol stack 340 each supports the mapping of network level, i.e., Internet Protocol (IP), data packets and characteristics onto underlying network protocols. In a presently preferred embodiment, the respective SNDCP layers 326 and 345 support the adaptation of IP data packets to over-the-air Logical Link Control (LLC) frames for transmission between a base station and a WM of a terminal. In the reverse, or alternative, transmission direction, the respective SNDCP layers 326 and 345 support the adaptation of LLC frames to

respective IP data packets, for subsequent transmission to IP gateways and/or IP data networks, via an access router.

The respective SNDCP layers 326 and 345 support the compression and decompression of message headers of packet data sent and received on the over-the-air interface between the respective WM and base station. The compression and decompression of message headers includes, but is not limited to, the compression and decompression of Internet Protocol (IP) data messages.

The SNDCP layer 326 of a wireless modem (WM) protocol stack 320 and the SNDCP layer 345 of a base station protocol stack 340 each further provide the mechanism for determining the length of a data message and its individual data packets, for subsequent use in the compression/decompression algorithms. Too, the respective SNDCP layers 326 and 345 support the functionality for providing the packet type, including, but not limited to, normal IP packet, full header packet and context state packet, to the requisite compression and decompression algorithms.

The SNDCP layer 326 of a wireless modem (WM) protocol stack 320 and the SNDCP layer 345 of a base station protocol stack 340 support quality of service, i.e., QoS, functionality for packet data transmissions. In a presently preferred embodiment, the QoS profile for bearer data traffic is a non real-time profile.

In a presently preferred embodiment, on the network side, the base station protocol stack 340 for the packet data bearer plane comprises a T1 interface layer 346 and a frame relay layer 347. In a presently preferred embodiment, the protocol stack 360 for an access router for the packet data bearer plane comprises a T1 interface layer 361, a frame relay layer 362 and an Internet Protocol (IP) layer 363.

A base station, or base transceiver station (BTS), supports an intra-BTS relay function, which relays packet data between the wireless modem – base station interface and the base station – access router interface. In the subscriber – network direction, i.e., upstream, the BTS bridge functionality extracts Internet Protocol (IP) packets from the Subnetwork Dependent Convergence Protocol (SNDCP) layer 345 and delivers them to the frame relay layer 347, for subsequent transmission to an access router. In the alternative direction, i.e., the network – subscriber, or downstream, direction, the BTS bridge functionality extracts IP packets from the frame relay layer 347 and deliv rs them to the SNDCP layer 345, for subsequent over-the-air transmission to a respective wireless modem (WM).

On the wireless modem (WM) – base station interface, the WM is instantiated at the transmission link layer via a Temporary Logical Link Identity (TLLI) address assigned to the WM. On the base station – network, i.e., access router, interface, each WM is instantiated at the transmission link layer via a frame relay switched virtual circuit (SVC). In a presently preferred embodiment, a BTS bridge function is to maintain the mapping between respective TLLIs and SVCs of a wireless modem (WM) of a respective terminal. In a presently preferred embodiment, this mapping, or bridging, is dynamically established as part of address assignment procedures executed on the two interfaces, i.e., the WM – base station interface and the base station – network, i.e., Subscriber Management Platform (SMP) interface, as part of the Customer Registration procedure 191 executed for a respective subscriber terminal.

Further, the BTS bridge functionality allows a base station to operate as a transmission link layer bridge that obviates the need for IP data transmission routing within the base station.

The respective T1 interface layers 346 and 361 of the base station protocol stack 340 and the access router protocol stack 360 are equivalent to the respective T1 interface layer 276 of the base station protocol stack 270 of Figure 12, except the T1 interface layers 346 and 361 support packet data, rather than signaling, traffic transmissions. The respective frame relay layers 347 and 362 of the base station protocol stack 340 and the access router protocol stack 360 are equivalent to the frame relay layer 277 of the base station protocol stack 270 of Figure 12, except the frame relay layers 347 and 362 support packet data, rather than signaling, traffic transmissions.

The access router IP layer 363 supports the network Internet Protocol (IP) for transmitting packet data to or from a data network, e.g., the Internet, through an access router, to a base station, and ultimately a subscriber station.

A presently preferred embodiment of a voice signaling plane architecture 490, shown in Figure 15, for use with a terminal comprising a wireless modem (WM), comprises a protocol stack 400 for the personal computer (PC) of an H.323 terminal, and a protocol stack 420 for a wireless modem (WM) of the respective H.323 terminal. The voice signaling plane architecture 490 also comprises a protocol stack 440 for a base station, or base transceiver station (BTS), a protocol stack 460 for an access router, and a protocol stack 480 for H.323 gateway/gatekeeper combinatory network nodes.

In a presently preferred embodiment, the protocol stack for a personal computer (PC) 400 comprises an H.245 protocol layer 401, a Q.931 protocol layer

402, an RAS protocol layer 402, a Transmission Control Protocol (TCP) layer 404, a User Datagram Protocol (UDP) layer 406, an Internet Protocol (IP) layer 405, a modem command layer 415 and a physical link layer 416. The respective physical link layer 416, modem command layer 415 and IP layer 405 of the PC protocol stack 400 are equivalent to the respective physical link layer 302, modem command layer 304 and IP layer 306 of the PC protocol stack 300 of Figure 14, except the physical link layer 416, modem command layer 415 and IP layer 405 support voice signaling, rather than packet data, traffic transmissions.

In a presently preferred embodiment, the H.323 gateway/gatekeeper protocol stack comprises an H.245 protocol layer 421, a Q.931 protocol layer 422, an RAS protocol layer 423, a Transmission Control Protocol (TCP) layer 424, a User Datagram Protocol (UDP) layer 425, an Internet Protocol (IP) layer 426, an ethernet layer 427 and a 10BaseT interface layer 428.

In a presently preferred embodiment, the voice signaling plane architecture 490 conforms to the H.323 standard for the upper transmission protocol layers and uses Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP) as the underlying transport and network protocols. Referring to Figure 15, all the voice signaling components, i.e., the respective H.245 protocol layers 401 and 421, the respective Q.931 protocol layers 402 and 422, and the respective registration admissions and status (RAS) protocol layers 403 and 423 are implemented in the PC of the subscriber H.323 terminal and the gateway and gatekeepers of the wireless access network.

The H.245 protocol layer 401 of the PC protocol stack 400 and the H.245 protocol layer 421 of the gateway/gatekeeper protocol stack 480 supports H.245 protocol end-to-end channel control, i.e., for transmission of voice signaling messages governing operation of the respective H.323 entities of the wireless access network. The H.245 protocol control messages govern operations including, but not limited to, capabilities exchange signaling, opening, or establishment, of a logical channel, closing, or de-allocation, of a logical channel, mode preference request signaling, flow control message signaling, and general command and indication signaling.

In a presently preferred embodiment, the H.245 signaling between two endpoints, e.g., two H.323 terminals, or an H.323 terminal and a switched circuit network, in a wireless access network, is routed through a gatekeeper, with the respective H.245 signaling messages carried over TCP/IP connections. The respective TCP layers 404 and 424 and the respective IP layers 405 and 426 of a terminal protocol stack 400 and a gateway/gatekeeper protocol stack 480 manage

the respective TCP/IP connections between a PC of an H.323 t rminal and a gateway/gatekeeper.

In a presently preferred embodiment, call, i.e., voice, control signaling is defined within the H.225.07 protocol, which is part of the H.323 protocol suite. H.225.0 incorporates the DSS-1 recommendation Q.931 protocol and defines the set of mandatory Q.931 control messages. Call control signaling between two endpoints, e.g., two H.323 terminals, or an H.323 terminal and a switched circuit network, of a wireless access network is routed by a gatekeeper, with the respective Q.931 signaling messages carried over TCP/IP connections. The respective TCP layers 404 and 424 and the respective IP layers 405 and 426 of a terminal protocol stack 400 and a gateway/gatekeeper protocol stack 480 manage the respective TCP/IP connections between a PC of an H.323 terminal and a gateway/gatekeeper.

Registration Admissions and Status (RAS) channels, as previously discussed with regard to Figure 3, carry control signaling messages, used in gatekeeper discovery, endpoint registration and endpoint status procedures. RAS protocol layer 403 of the terminal protocol stack 400 and RAS protocol layer 423 of the H.323 gateway/gatekeeper protocol stack 480 also support the protocols for subscriber authentication within a wireless access network, in the voice signaling plane.

RAS signaling is between an endpoint, i.e., an H.323 terminal or a switched circuit network, and a gatekeeper of the wireless access system. In a presently preferred embodiment, RAS control messages are carried over UDP/IP channels. The respective UDP layers 406 and 425 and the respective IP layers 405 and 426 of a terminal protocol stack 400 and a gateway/gatekeeper protocol stack 480 manage the respective UDP/IP connections between a PC of an H.323 terminal and a gateway/gatekeeper.

In a presently preferred embodiment, on the network side, the protocol stack 460 for an access router in the voice signaling plane architecture 490 comprises an Internet Protocol (IP) layer 433, an ethernet layer 431 and a 10BaseT interface layer 432. As the wireless access system supports IP packet voice, i.e., IP telephony, calls, the IP layer 433 of the access router protocol stack 460 and the IP layer 426 of the H.323 gateway/gatekeeper protocol stack 480 support the Internet Protocol (IP) for the respective voice signaling traffic.

An access router and gateway or gatekeeper transmit voice signaling messages between them via ethernet protocols. The respective ethernet layers

431 and 427 of the access router protocol stack 460 and H.323 gateway/gatekeeper stack 480 support the ethernet transmission protocols.

The 10BaseT interface layer 432 of the access router protocol stack 460 and the 10BaseT interface layer 428 of the H.323 gateway/gatekeeper protocol stack 480 comprise the protocols and procedures for managing a physical 10BaseT communication interface between the respective access router and the H.323 gateway and/or H.323 gatekeeper. The 10BaseT communication interface is a standard wireline interface. In the voice signaling plane specifically, the respective 10BaseT interface layers 432 and 428 are used to transmit voice signaling information, or messages, between the respective access router and the H.323 gateway and/or H.323 gatekeeper.

The subscriber side of the access router protocol stack 460 is comprised of layers that are equivalent to those of the access router protocol stack 360 of Figure 14, except that the layers in the access router protocol stack 460 support voice signaling, rather than packet data, traffic transmissions.

The layers of the wireless modem (WM) protocol stack 420 are equivalent to the WM protocol stack 320 layers of Figure 14, except that the WM protocol stack 420 layers support voice signaling, rather than packet data, traffic transmissions. Likewise, the layers of the base station protocol stack 440 are equivalent to the base station protocol stack 340 layers of Figure 14, except the base station protocol stack 440 layers support voice signaling, rather than packet data, traffic transmissions.

A presently preferred embodiment of a voice bearer plane architecture 500, shown in Figure 16, comprises a protocol stack 510 for the personal computer (PC) of an H.323 terminal, and a protocol stack 525 for a wireless modem (WM) of the respective H.323 terminal. The voice bearer plane architecture 500 also comprises a protocol stack 540 for a base station, or base transceiver station (BTS), a protocol stack 560 for an access router, and a protocol stack 580 for an H.323 gateway.

In a presently preferred embodiment, the protocol stack 510 for a personal computer (PC) comprises a vocoder layer 501, a Real Time Protocol (RTP) layer 502, a User Datagram Protocol (UDP) layer 503, an Internet Protocol (IP) layer 504, a modem command layer 505 and a physical link layer 506.

The physical link layer 506, modem command layer 505 and IP layer 504 of the PC protocol stack 510 are equivalent to the respective physical link layer 302, modem command layer 304 and IP layer 306 of the PC protocol stack 300 of

Figure 14, except the physical link layer 506, modem command layer 505 and IP layer 504 support voice, rather than packet data, traffic transmissions.

In a presently preferred embodiment, the protocol stack 580 for an H.323 gateway comprises a vocoder layer 507, an RTP layer 508, a UDP layer 509, an IP layer 511, an ethernet layer 512 and a 10BaseT layer 513.

The Internet Protocol (IP) layer 511, ethernet layer 512 and 10BaseT layer 513 of the H.323 gateway protocol stack 580 are equivalent to the respective IP layer 426, ethernet layer 427 and 10BaseT layer 428 of the H.323 gateway/gatekeeper protocol stack 480 of Figure 15, except the IP layer 511, ethernet layer 512 and 10BaseT layer 513 support bearer voice, rather than voice signaling, traffic transmissions.

The PC protocol stack 510 comprises a vocoder layer 501 and the H.323 gateway protocol stack 580 comprises a vocoder layer 507 for supporting voice encoding/decoding. The respective vocoder layers 501 and 507 each comprise audio coder/decoder functionality. In a presently preferred embodiment, the respective vocoder layers 501 and 507 are capable of encoding and decoding voice, i.e., speech, according to ITU-T recommendation G.711. In alternative embodiments, the respective vocoder layers 501 and 507 may comprise, or additionally comprise, functionality for encoding and decoding speech using ITU-T recommendations, including, but not limited to, the G.722 protocol, the G.728 protocol, the G.729 protocol, the MPEG 1 audio protocol and the G.723.1 protocol.

In a presently preferred embodiment, the vocoder layer 501 of the PC protocol stack 510 and the vocoder layer 507 of the H.323 gateway protocol stack 580 are capable of transmitting and receiving A-law and μ-law coding, i.e., A-law and μ-law encoded voice transmissions.

In a presently preferred embodiment, the audio algorithm used by the encoder functionality of the vocoder layer 501 of the PC protocol stack 510 and the vocoder layer 507 of the H.323 gateway protocol stack 580 are derived via the Capability Exchange procedure 854, as further discussed with regard to Figure 4, executed over the respective H.245 voice signaling channel between the respective H.323 terminal and H.323 gateway, via an H.323 gatekeeper.

The Real Time Protocol (RTP) layer 502 of the PC protocol stack 510 and the RTP layer 508 of the H.323 gateway protocol stack 580 each comprise respective protocol functionality for transporting voice messages, or packets or stream, within the wireless access network, between an H.323 terminal and an H.323 gateway.

In a presently preferred embodiment, RTP voice packets can be carried over an unreliable channel, and, thus, are supported by a User Datagram Protocol/Internet Protocol (UDP/IP) connection. The UDP layer 503 and IP layer 504 of the PC protocol stack 510 and the UDP layer 509 and IP layer 511 of the H.323 gateway protocol stack 580 support the UDP/IP protocol connections for the respective RTP voice packet transmissions between a respective H.323 terminal and an H.323 gateway.

The Real Time Protocol (RTP) carries audio, i.e., voice, information, or messages, in frames. In a presently preferred embodiment, before a bearer channel for voice transmissions is opened, or established, the maximum number of frames per IP transmission packet is established by H.245 signaling messages between an H.323 terminal and an H.323 gateway or H.323 gatekeeper, in the voice signaling plane. H.323 voice receiving entities signal the maximum number of audio frames they are capable of accepting via a single IP packet voice transmission. The respective H.323 transmitting entity thereafter may send any whole number of audio frames to the H.323 receiving entity, in each IP packet voice transmission, up to the maximum number of frames signaled by the H.323 receiving entity. In a presently preferred embodiment, H.323 transmitters do not split audio frames across IP packet voice transmissions.

The layers of the WM protocol stack 525 are generally equivalent to the WM protocol stack 420 layers of Figure 15, except the WM protocol stack 525 layers support bearer voice, rather than voice signaling, traffic transmissions. The layers of the base station protocol stack 540 are generally equivalent to the base station protocol stack 440 layers of Figure 15, except the base station protocol stack 540 layers support bearer voice, rather than voice signaling, traffic transmissions.

The SNDCP layer 521 of the WM protocol stack 525 and the SNDCP layer 522 of the base station protocol stack 540, for the voice bearer plane, support the compression and decompression of message headers of packet voice messages sent and received on the over-the-air interface between the respective WM and base station. The compression and decompression of message headers includes, but is not limited to, the compression and decompression of Real Time Protocol (RTP) data messages, User Datagram Protocol (UDP) data messages, and Internet Protocol (IP) data messages.

In a presently preferred embodiment, an end user computing device, e.g., a PC, may use an RTP/UDP/IP protocol stack for packet voice transmissions. However, with the introduction of RTP, there is concern that the twelve-byte RTP

message header is too large for a twenty-byte network, when the underlying physical transmission link is a low-throughput type. With the additional UDP and IP message headers, the total message header overhead per voice packet can become forty bytes. This, in turn, can translate into a thirty-three percent bandwidth efficiency, which may be very low, and actually intolerable, on a low-throughput transmission link, for example, e.g., a wireless, over-the-air, link.

A compression algorithm for compressing, and subsequently decompressing, an RTP/UDP/IP message header is valuable in terms of increasing the wireless link efficiency of a wireless access network. An Internet draft, draft-ietf-avt-crtp-04.txt, specifies a mechanism for this purpose and is included herein by reference, as if fully incorporated herein. The existing Internet compression algorithm draft is similar to the TCP/IP compression algorithm by Van Jacobson, and provides a mechanism for compressing a forty-byte message header into two to four bytes. Further, the existing Internet compression algorithm draft is designed to operate on a link-by-link basis, and, thus, provides flexibility within the system for managing packet voice transmissions.

In a presently preferred embodiment, the compression algorithm supported by the respective SNDCP layers 521 and 522, for over-the-air packet voice transmissions, is based on the fact that a number of fields in an RTP/UDP/IP protocol message header do not change from packet voice to packet voice, for an entire voice message. After transmitting the uncompressed message header once, for, e.g., a first packet voice of a voice message, the consistent fields may thereafter be omitted from succeeding compressed headers of subsequent packet voice of the voice message.

Another compression factor of the respective SNDCP layers 521 and 522 supported compression algorithm is that the difference from packet voice to packet voice of a voice message is often constant. Therefore, if the uncompressed RTP/UDP/IP message header is maintained, along with the expected constant difference at the receiving entity, the transmitting entity need only thereafter send an uncompressed header if there is any change in the constant difference.

The SNDCP layer 521 of a wireless modem (WM) protocol stack 525 and the SNDCP layer 522 of a base station protocol stack 540 each further provide the mechanism for determining the length of a voice message and its individual voice packets, for subsequent use in the compression/decompression algorithms. Too, the respective SNDCP layers 521 and 522 support the functionality for providing the packet type, including, but not limited to, normal IP packet, full header packet,

compressed UDP packet, compressed RTP packet, and context state packet, to the requisite compression and decompression algorithms.

The SNDCP layer 521 of a wireless modem (WM) protocol stack 525 and the SNDCP layer 522 of a base station protocol stack 540 support quality of service, i.e., QoS, functionality for packet voice transmissions. In a presently preferred embodiment, the QoS profile for bearer voice traffic is a non real-time profile.

The layers of the access router protocol stack 560 are equivalent to the access router protocol stack 460 layers of Figure 15, except the access router protocol stack 560 layers support bearer voice, rather than voice signaling, traffic transmissions.

As previously discussed with reference to Figures 12, 14, 15 and 16, the wireless modem (WM) of a terminal or H.323 terminal and a base station each have protocol stacks that comprise a Logical Link Control (LLC) layer. The LLC layers of the respective WM protocol stacks and base station protocol stacks provide a reliable, radio-independent, logical link for communications between the respective wireless modem (WM) and base station. More specifically, the LLC layers of the respective WM protocol stacks and base station protocol stacks support a variety of procedures, or functions, 710 for logical link control, as shown in Figure 17.

The respective LLC layers functionality 710 comprises a procedure 712 for the establishment, and subsequent release, of LLC links between a WM and a base station. The LLC links are used for communication transmissions between a subscriber terminal, or subscriber H.323 terminal, and a base station, for the transmission of bearer traffic, voice or data, and signaling traffic between the subscriber terminal, or subscriber H.323 terminal, and the base station.

The LLC layers functionality 710 also comprises a procedure 714 for the transfer, or transmission, of bearer traffic, data or voice, between a WM and a base station. The LLC layers procedures 710 further comprise a procedure 716 for the transfer, or transmission, of packet data or voice signaling traffic, for communication channel establishment, maintenance, statusing and release, between a WM and a base station. The procedure 714 for the transmission of bearer data and the procedure 716 for the transmission of signaling traffic each comprise unacknowledged point-to-point message transmissions between a WM and a base station. The procedure 714 for the transmission of bearer data and the procedure 716 for the transmission of signaling traffic also each comprise

acknowledged, reliable, point-to-point message transmissions between a WM and a base station.

The respective LLC layers of a WM protocol stack and of a base station protocol stack also comprise a procedure 718 for detecting and recovering from lost or corrupted transmitted Logical Link Control (LLC) frames, or messages. The LLC layers functionality 710 further comprises a procedure 720 for controlling the transmission flow of LLC frames between a WM and a base station. The LLC layers procedures 710 also comprise a procedure 722 for supporting encryption and decryption functionality for LLC frames transmitted between a WM and a base station.

As previously described, with reference to Figure 1, the wireless access network provides network management services 6, which are used to manage the network elements, or nodes, of the network, for example, but not limited to, base stations, access routers, gateways and gatekeepers. In a presently preferred embodiment, the management of the respective network nodes is accomplished using internet-based protocols including, but not limited to, the Simple Network Management Protocol (SNMP) and the File Transfer Protocol (FTP). Network node management is managed via the Network Node Management platform 172, as described with reference to Figure 6.

In a presently preferred embodiment, a direct network node management approach is used that allows management of any network node having an Internet Protocol (IP) address. Network node management may be accommodated, or otherwise accomplished, from a variety of locations, including but not limited to, a remote network operations center, which supports a main centralized management location, the Internet, which provides limited remote management capabilities due to Internet fire walls, and/or local management provisioning at node installation.

Presently preferred embodiments of a generic protocol stack 600 for a node manager, either remote or local, and a protocol stack 620 for a network node, or element, e.g., a base station, an access router, a gateway, or a gatekeeper, as shown in Figure 18, comprise respective Simple Network Management Protocol (SNMP) layers 602 and 603 for supporting the Simple Network Management Protocol (SNMP). The File Transfer Protocol (FTP)/Multicast File Transfer Protocol (MFTP) layer 604 of the node manager protocol stack 600 and the FTP/MFTP layer 605 of the node protocol stack 620 support a choice of either the File Transfer Protocol (FTP) or the Multicast File

Transfer Protocol (MFTP) 604 for file transfers between the node manager and the respective node.

Underlying the management usage protocols, i.e., the SNMP, the FTP and the MFTP, is a Transmission Control Protocol (TCP)/Internet Protocol (IP), TCP/IP, connection, for the transfer of management data requiring a secure, i.e., reliable, transmission channel. The respective TCP layer 606 and IP layer 608 of the node manager protocol stack 600 and the respective TCP layer 607 and IP layer 609 of the node protocol stack 620 support the secure TCP/IP connections.

Also underlying the management usage protocols is a User Datagram Protocol (UDP)/Internet Protocol (IP), UDP/IP, connection, for the transfer of management data that can be transmitted over an unreliable channel. The respective UDP layer 610 and IP layer 608 of the node manager protocol stack 600 and the respective UDP layer 611 and IP layer 609 of the node protocol stack 620 support the unsecure UDP/IP connections.

The sub-network protocol layers 612 of the node manager protocol stack 600 and the sub-network protocol layers 613 of the node protocol stack 620 support underlying transmission protocols comprising a physical transmission layer protocol.

The manager applications layer 614 of the node manager protocol stack 600 supports the application functionality for network node management, including, but not limited to, configuration management, fault management, performance management, accounting management and security management. Likewise, the agent applications layer 615 of the node protocol stack 620 supports the application functionality for network node management, including, but not limited to, configuration management, fault management, performance management, accounting management and security management.

The use of a direct management scheme from a centralized network operations location can lead to a heavy processing load on the Network Node Management platform 172. The processing load on the Network Node Management platform 172 can be further increased due to the simplicity of the mechanisms used in the Simple Network Management Protocol (SNMP) and the need generally for frequent polling to detect SNMP mechanism failures. A presently preferred embodiment solution to the processing load problem is the maintenance of a hierarchy of management platforms for network node management, as shown in Figure 19.

In the management hierarchy system 630 of Figure 19, one manager of managers 632 of the management system is designated. In a presently preferred

embodiment, the manager of managers 632 is the Network Node Management platform 172 of Figure 6. The manager of managers 632 manages two or more node managers 634. In a presently preferred, a node manager 634 can comprise a gateway management platform 162, a router management platform 164 or a wireless access network management platform 166. Each node manager 634, in turn, manages two or more network nodes 636. The network nodes 636 comprise base stations, access routers, wireless router and concentrator (WRC), gateways and gatekeepers of the wireless access network.

In a presently preferred embodiment, switched circuit network gateway nodes are managed from the network hierarchy system 630 using the Simple Network Management Protocol (SNMP) and the File Transfer Protocol (FTP). In an alternative embodiment, switched circuit network gateway nodes comprise their own internal management system, which is thereafter integrated into a common operations center local area network (LAN). In this alternative embodiment, the common operations center LAN further comprises the network hierarchy system 630, for the remainder of the network node types.

In a presently preferred embodiment, access router nodes are managed from the network hierarchy system 630 using the Simple Network Management Protocol (SNMP) and the File Transfer Protocol (FTP).

Referring to Figure 20, in a presently preferred embodiment, base station network nodes and Customer Premises Radio Unit (CPRU) network nodes are managed from a customized general purpose wireless access management platform 640, also known as a wireless access network management platform 166, as discussed with reference to Figure 6. The wireless access management platform 640 manages the respective base stations 642 and CPRUs 644 of the wireless access network via an Internet Protocol (IP) network, or sub-network, 646. In a presently preferred embodiment, the wireless access management platform 640 uses both unicast 641, i.e., point-to-point, and multicast 643, i.e., point-to-multipoint, IP services for management of the base stations 642 and CPRUs 644 of the respective wireless access network.

In a presently preferred embodiment, the Simple Network Management Protocol (SNMP) is used for the network management of the various base stations 642 and CPRUs 644 and the SNMP utilizes the Multicast File Transfer Protocol (MFTP) for file transfers between the wireless access management platform 640 and the respective base stations 642 and CPRUs 644.

Underlying the SNMP/MFTP protocol layers for base station and CPRU management is a Transmission Control Protocol (TCP)/Internet Protocol (IP),

TCP/IP, connection, for the transfer of management data requiring a secure, i.e., reliable transmission channel. Also underlying the SNMP/MFTP protocol layers for base station and CPRU management is a User Datagram Protocol (UDP)/Internet Protocol (IP), UDP/IP, connection, for the transfer of management data that can be transmitted over an unreliable, i.e., unsecure, channel.

A presently preferred embodiment of a base station management architecture 650, shown in Figure 21A, comprises a protocol stack 652 for a wireless access management platform 640, a protocol stack 654 for a first access router, a protocol stack 656 for a second access router, and a protocol stack 658 for a base station, or base transceiver station.

As the wireless access management platform 640 uses the Simple Network Management Protocol (SNMP) and the Multicast File Transfer Protocol (MFTP) to manage a respective base station, both the wireless access management platform protocol stack 652 and the base station protocol stack 658 comprise respective SNMP layers 652 and 651 and respective MFTP layers 654 and 655.

As previously discussed, underlying the management usage protocols, i.e., SNMP/MFTP, are Transmission Control Protocol (TCP)/Internet Protocol (IP), TCP/IP, connections for the transfer of management data requiring a secure, i.e., reliable, transmission channel. Thus, both the wireless access management platform protocol stack 652 and the base station protocol stack 658 comprise respective TCP layers 656 and 657 and respective IP layers 660 and 661. As also previously discussed, underlying the management usage protocols are User Datagram Protocol (UDP)/Internet Protocol (IP), UDP/IP, connections for the transfer of management data that can be transmitted over an unreliable, i.e., unsecure, transmission channel. Thus, both the wireless access management platform protocol stack 652 and the base station protocol stack 658 further comprise respective UDP layers 658 and 659.

In a presently preferred embodiment, the wireless access management platform 640 communicates with an access router via an ethernet local area network. Thus, both the wireless access management platform protocol stack 652 and the first router, i.e., the router communicating with the wireless access management platform 640, protocol stack 654 comprise respective ethernet layers 668 and 669.

In a presently preferred embodiment, frame relay is used as the link layer transport protocol between a base station and the wireless access network, including the network's wireless access management platform 640. Thus, the protocol stack of each respective access router in the transmission chain between

a base station and the wireless access management platform 640, e.g., protocol stack 654 and protocol stack 656, comprises a respective frame relay layer 662 and 663. Further, the protocol stack 658 of a base station and the protocol stack, e.g., 656, of an access router communicating with the base station each comprise a respective frame relay layer 687 and 657.

The communication between a base station and the wireless access network, including the network's wireless access management platform 640, relies on the Internet Protocol (IP). Thus, the wireless access management platform protocol stack 652, the base station protocol stack 658 and the access router protocol stacks 654 and 656 of the access routers in the transmission chain between the wireless access management platform 640 and the base station comprise respective IP layers 660, 661, 670 and 671.

A presently preferred embodiment of a Customer Premises Radio Unit (CPRU) management architecture 680, shown in Figure 21B, comprises a protocol stack 652 for a wireless access management platform 640, a protocol stack 654 for a first access router, a protocol stack 656 for a second access router, a protocol stack 682 for a base station, and a protocol stack 684 for a CPRU.

In a presently preferred embodiment, a base station and a CPRU communicate via a physical radio interface, and thus, the base station protocol stack 682 and the CPRU protocol stack 684 each comprise a respective radio layer 685 and 686 for managing the radio, i.e., wireless, or over-the-air, interface between them.

The base station protocol stack 682 and the CPRU protocol stack 684 also each comprise respective radio link control/medium access control (RLC/MAC) layers 689 and 688, logical link control (LLC) layers 691 and 690 and Subnetwork Dependent Convergence Protocol (SNDCP) layers 693 and 692.

The MAC function of the respective RLC/MAC layers 689 and 688 for the base station protocol stack 682 and the CPRU protocol stack 684 provides signal message multiplexing on both uplink and downlink channels of the over-the-air interface between the respective base station and respective CPRU. The RLC function of the respective RLC/MAC layers 689 and 688, for its part, provides a radio-dependent reliable link between the respective base station and the respective CPRU. The RLC functions of the base station and the CPRU it communicates with are responsible for the transfer, or transmission, of logical link control (LLC) frames of information on the over-the-air interface between them.

The respective LLC layers 691 and 690 of the base station protocol stack 682 and the CPRU protocol stack 684 provide a reliable, radio-independent, logical link for communications between the respective base station and the respective CPRU. The respective Subnetwork Dependent Convergence Protocol (SNDCP) layers 693 and 692 of the base station protocol stack 682 and the CPRU protocol stack 684 support the mapping of network level, i.e., Internet Protocol (IP), signaling messages onto the underlying network and transmission protocols.

The Simple Network Management Protocol (SNMP) layer 734, the Multicast File Transfer Protocol (MFTP) layer 732, the User Datagram Protocol (UDP) layer 733, the Transmission Control Protocol (TCP) layer 731 and the Internet Protocol (IP) layer 730 of the CPRU protocol stack 684 are equivalent to the respective SNMP layer 651, the respective MFTP layer 655, the respective UDP layer 659, the respective TCP layer 657 and the respective IP layer 661 of the base station protocol stack 658 of Figure 21A, except that the SNMP layer 734, the MFTP layer 732, the UDP layer 733, the TCP layer 731 and the IP layer 730 comprise the Customer Radio Premises Unit (CPRU) protocol stack 684, rather than a base station protocol stack.

The frame relay layer 656 of the base station protocol stack 682 is equivalent to the frame relay layer 656 of the base station protocol stack 658 of Figure 21A. Further, the wireless access management protocol stack 652 is equivalent to the wireless access management protocol stack 652 of Figure 21A, the first router protocol stack 654 is equivalent to the first router protocol stack 654 of Figure 21A and the second router protocol stack 656 is equivalent to the second router protocol stack 656 of Figure 21A.

A presently preferred embodiment of the network components, or elements or nodes, 750 required for end-to-end packet bearer, voice and data, transmissions, as shown in Figure 22, is comprised of a frame relay network 755 and one or more sub-networks A 751.

In an embodiment, the network components 750 for end-to-end packet bearer transmissions also comprise one or more sub-networks B 752, if the network comprises one or more Customer Premises Radio Units (CPRUs) 753. In a presently preferred embodiment, a sub-network B 752 is a local area network (LAN). In a presently preferred embodiment, a sub-network B 752 supports ethernet protocol transmissions.

The frame relay network 755 comprises one or more access routers 754 providing connectivity to one or more data network , e.g., Internet, gateways 756,

and thus to one or more data networks 757, including the Internet. An access router 754 also provides connectivity to one or more other access routers, or routers, e.g., router 758. Router 758 supplies the network connection, or connectivity, to one or more voice, e.g., H.323, gateways, or voice, e.g., H.323, gateway/gatekeeper combinations 759, for access to one or more switched circuit networks.

A sub-network A 751 connects the access router 754 to one or more base stations 760. Each base station 760, in turn, provides connectivity to one or more wireless modems (WM) 761 and/or one or more Customer Premises Radio Units (CPRUs) 753, via an over-the-air interface. Each wireless modem (WM) 761 is connected to a computing device 762, for example, but not limited to, e.g., a personal computer (PC), a smart terminal, a palm pilot or a workstation. In a presently preferred embodiment, a WM 761 and respective computing device 762 comprise a terminal.

If a CPRU 753 is included in the wireless access network, a sub-network B 752 comprises the respective CPRU 753 connected to one or more computing devices 763, for example, but not limited to, a personal computer (PC), a smart terminal or a workstation.

An access router 754 performs direct routing of bearer traffic to a computing device 762 via a respective WM 761, on a sub-network A 751, based on an IP address assigned to the respective WM 761.

An Address Resolution Protocol (ARP) table within the access router 754 provides the association between the IP address of a respective WM 761 or CPRU 753 and the frame relay virtual circuits (VCs) used for bearer traffic transmissions between the access router 754 and a base station 760. Individual virtual circuits (VCs) are also established between the access router 754 and each sub-network A 751 destination, i.e., each WM 761 and each CPRU 753.

On the over-the-air interface, i.e., between a base station 760 and a WM 761 or CPRU 753, bearer traffic, voice and data, is encapsulated and tunneled over a logical link control (LLC) link between a base station 760 and a WM 761 or a CPRU 753. A base station bridging table provides the association between the respective virtual circuit (VC), for transmission of the bearer traffic between an access router 754 and a respective base station 760, and the respective temporary logical link identity (TLLI) assigned to a WM 761 or a CPRU 753, for message transmission on the over-the-air interface between the base station and the WM 761 or CPRU 753.

As a WM 761 supports a computing device 762 on a sub-network A 751, the WM 761 provides a direct addressing link to the respective computing device 762.

For computing devices 763 on a sub-network B 763, an access router 754 directs routing of bearer traffic to the respective CPRU 753, based on an IP address assigned to the respective CPRU 763. The CPRU 753 thereafter is responsible for routing the bearer data to the respective computing device 763 on the respective sub-network B 752. An Address Resolution Protocol (ARP) table in the CPRU 763 provides the association between the IP address of the respective CPRU 763 and the ethernet address used for transmissions between the CPRU 753 and a respective computing device 763.

A presently preferred embodiment of the network components, or elements or nodes, 775 required for end-to-end signaling transmissions for terminal authentication and subscriber management, as shown in Figure 23, is comprised of a frame relay network 780 and one or more sub-networks A 785. The frame relay network 755 comprises one or more access routers 776. Each access router 776 provides connectivity to one or more other access routers, or routers 777. A router 777, in turn, is connected to the Subscriber Management Platform (SMP) 182 of the Operations Support System (OSS). A sub-network A 785 comprises an access router 776 and one or more base stations 779.

The access router 776 performs direct routing of terminal authentication and subscriber management signaling to a base station 779, based on the base station's IP address. An Address Resolution Protocol (ARP) table within the access router 776 provides the association between the IP address of the base station 779 and the frame relay virtual circuits (VCs) used for transmissions between the access router 776 and the respective base station 779. Each base station 779 requires a single virtual circuit (VC) for terminal authentication and subscriber management signaling. In a presently preferred embodiment, the single virtual circuit (VC) assigned to a base station 779 for terminal authentication and subscriber management signaling may also be used for network management system traffic.

A presently preferred embodiment of the network components 800 required for end-to-end network management transmissions for node and accounting management, as shown in Figure 24, is comprised of a frame relay network 810 and one or more sub-networks 805. The frame relay network 810 comprises one or more access routers. Each access router 801 is connect d to one or more other access routers, or routers 802. A first router 802 provides connectivity to an

external network 803. A second router 802 provides connectivity to the Subscriber Management Platform (SMP) 182 and the Network Node Management Platform 172 of the wireless access network. In a presently preferred embodiment, the SMP 182 and the Network Node Management Platform 172 reside on an operations local area network (LAN) 809.

A sub-network 805 comprises an access router 801, one or more base stations 807 and, in an embodiment, one or more Customer Premises Radio Units (CPRUs) 808.

An access router 801 performs direct routing of accounting and node management messages to a base station 807, or CPRU 808, based on the respective base station's or CPRU's IP address. An Address Resolution Protocol (ARP) table within the access router 801 provides the association between the IP address of the base station 807 or CPRU 808 and the frame relay virtual circuit (VC) used for accounting and node management signaling message transmissions between the access router 801 and the respective base station 807 or respective CPRU 808. Each base station 807 requires a single virtual circuit (VC) for accounting and node management messages. In a presently preferred embodiment, the single VC assigned to a base station 807 may also be used for terminal authentication and subscriber management signaling. Each CPRU 808 also requires a single virtual circuit (VC) for accounting and node management messages.

While embodiments are disclosed herein, many variations are possible which remain within the spirit and scope of the inventions. Such variations are clear upon inspection of the specification, drawings and claims herein. The inventions therefore are not to be restricted except by the scope of the appended claims.

Claims

1. A telecommunications system supporting wireless access, comprising:

a computing device;

a wireless modem connected to said computing device;

a base station, wherein said base station and said wireless modem communicate via an over-the-air interface, and wherein said over-the-air interface supports a wide area wireless protocol;

an access router, wherein said base station and said access router communicate via a first interface;

a gateway, wherein said access router and said gateway communicate via a second interface and said gateway further communicates with a data network via a third interface; and

an H.323 gateway, wherein said access router and said H.323 gateway communicate via a fourth interface and said H.323 gateway further communicates with a switched circuit network via a fifth interface.

2. The telecommunications system of claim 1, wherein said computing device comprises a personal computer and said computing device and said wireless modem comprise a terminal.

3. The telecommunications system of claim 2, wherein said telecommunications system further comprises more than one base station and said terminal comprises a transportable terminal, and wherein said transportable terminal may communicate with a first base station at a first time and a second base station at a second time.

4. The telecommunications system of claim 2, wherein said wireless modem is installed in said personal computer, and said wireless modem and said personal computer comprise a transportable terminal.

5. The telecommunications system of claim 2, wherein said terminal is allocated a first internet protocol (IP) address for communicating within said telecommunications system and said base station is allocated a second internet protocol (IP) address for communicating within said telecommunications system.

6. The telecommunications system of claim 2, wherein said gateway transmits a packet data message from said data network to said access router, said access router transmits said packet data message to said base station and said base station transmits said packet data message to said terminal.

7. The telecommunications system of claim 1, wherein said third interface comprises a wireline interface and said fifth interface comprises a wireline interface.

8. The telecommunications system of claim 1, further comprising a telephone connected to said computing device, wherein said telephone and said computing device and said wireless modem comprise an H.323 terminal.

9. The telecommunications system of claim 8, wherein said H.323 gateway transmits a voice message from said switched circuit network to said access router, said access router transmits said voice message to said base station and said base station transmits said voice message to said H.323 terminal.

10. The telecommunications system of claim 1, wherein said data network comprises the Internet.

11. The telecommunications system of claim 1, wherein said switched circuit network comprises a public system telephone network.

12. A telecommunications system supporting wireless access, comprising:

a computing device capable of receiving packet data;

a radio unit capable of receiving packet transmissions on an over-the-air interface, wherein said radio unit is connected to said computing device; and

a wireless access network capable of communicating with a packet data network, said wireless access network further capable of communicating with a switched circuit network, wherein said wireless access network communicates with said radio unit via a wireless interface, and wherein said wireless interface supports a wide area wireless protocol.

13. The telecommunications network of claim 12, further comprising a voice access device capable of receiving a voice message, wherein said voice

access device is connected to said computing device, and wherein said computing device, said voice access device and said radio unit comprise an H.323 terminal.

14. The telecommunications network of claim 13, wherein said radio unit comprises a wireless modem, and wherein said computing device and said wireless modem comprise a transportable terminal.

15. The telecommunications network of claim 13, wherein said computing device comprises a personal computer and said voice access device comprises a telephone.

16. The telecommunications network of claim 12, further comprising a voice access device capable of receiving a voice message, wherein said voice access device is connected to said radio unit, and wherein said voice access device and said radio unit comprise an H.323 terminal.

17. The telecommunications network of claim 16, wherein said radio unit comprises a Customer Premises Radio Unit (CPRU), and wherein said computing device and said CPRU comprise a terminal.

18. The telecommunications network of claim 16, wherein said computing device comprises a personal computer and said voice access device comprises a telephone.

19. The telecommunications network of claim 12, further comprising an H.323 gateway, said H.323 gateway comprising the capability to communicate with said wireless access network via a first interface, and further comprising the capability to communicate with said switched circuit network via a second interface, wherein said H.323 gateway receives a switched circuit protocol message on said second interface from said switched circuit network, said H.323 gateway converts said switched circuit protocol message to an Internet Protocol message, and said H.323 gateway transmits said Internet Protocol message to said wireless access network on said first interface.

20. The telecommunications network of claim 12, wherein said data network comprises the Internet.

21. The telecommunications network of claim 12, wherein said switched circuit network comprises a public system telephone network.

22. A wireless access network for supporting both switched circuit message transmissions and packet data message transmissions, wherein one or more subscribers subscribe to the services of said wireless access network, and wherein said wireless access network supports a wide area wireless protocol, said wireless access network comprising:

a protocol for packet data message transmissions from a data network to a subscriber terminal;

a protocol for voice message transmissions from a switched circuit network to a subscriber H.323 terminal;

a protocol for fax transmissions from a switched circuit network to a subscriber terminal;

a protocol for security management of said wireless access network;

a protocol for the management of one or more network elements of said wireless access network;

a protocol for the management of subscriber information; and

a protocol for managing the billing of said one or more subscribers of said wireless access network.

23. The wireless access network of claim 22, wherein said protocol for packet data message transmissions comprises point-to-point transmission capabilities.

24. The wireless access network of claim 23, wherein said point-to-point transmission capabilities comprise an acknowledge transfer mechanism.

25. The wireless access network of claim 22, wherein said protocol for packet data message transmissions comprises point-to-multipoint transmission capabilities.

26. The wireless access network of claim 22, wherein said protocol for packet data message transmissions comprises the Internet Protocol.

27. The wireless access network of claim 22, wherein said protocol for voice message transmissions comprises the H.323 protocol overlaid on the Internet Protocol.

28. The wireless access network of claim 22, wherein said protocol for fax transmissions comprises the Internet Protocol.

29. The wireless access network of claim 22, wherein said protocol for security management comprises a terminal authentication functionality.

30. The wireless access network of claim 29, wherein said protocol for security management further comprises user identity confidentiality functionality, said user identity confidentiality functionality comprising a procedure for preventing tracing of a location of a subscriber of said wireless access network.

31. The wireless access network of claim 29, further comprising an over-the-air interface, and wherein said protocol for security management further comprises user information confidentiality functionality, said user information confidentiality functionality comprising a procedure for maintaining confidentiality of voice message transmissions and packet data message transmissions transmitted on said over-the-air interface of said wireless access network.

32. The wireless access network of claim 22, wherein said protocol for management of one or more network elements of said wireless access network comprises configuration management functionality and fault management functionality.

33. The wireless access network of claim 32, wherein a network element of said one or more network elements comprises a base station.

34. The wireless access network of claim 22, wherein said protocol for the management of subscriber information comprises functionality for management of a subscriber profile for each said subscriber of said wireless access network, and wherein a subscriber profile comprises a Quality of Service level assigned to each said subscriber.

35. The wireless access network of claim 22, wherein said protocol for managing the billing of said one or more subscribers of said wireless access network comprises a mechanism for charging a subscriber for wireless access, a mechanism for charging a subscriber for packet data message transmissions to and from said subscriber via said wireless access network and a mechanism for charging a subscriber for voice message transmissions to and from said subscriber via said wireless access network.

36. A wireless access network, wherein said wireless access network supports a wide area wireless protocol, said wireless access network comprising a wireless modem, wherein said wireless modem comprises a wireless modem protocol stack, said wireless modem protocol stack comprising:

a radio physical layer for communicating with a base station;

a radio link control layer for communicating with a base station;

a medium access control layer for communicating with a base station;

a logical link control layer for communicating with a base station; and

a subnetwork dependent convergence protocol layer for communicating with a base station.

37. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises one or more protocols comprising the General Packet Radio Service (GPRS) and General System for Mobile communication (GSM) protocols.

38. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a Global System for Mobile communication (GSM)/Enhanced Data rates for GSM Evolution (EDGE) radio interface.

39. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a Digital AMPS (DMAPS) radio interface.

40. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a IS-95 radio interface.

41. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a DECT radio interface.

42. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a WB-CDMA radio interface.

43. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a WB-TDMA radio interface.

44. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a IS-661 radio interface.

45. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a PCS radio interface.

46. The wireless access network of claim 36, wherein said radio physical layer of said wireless modem protocol stack comprises a procedure for transmission on a PACS radio interface.

47. The wireless access network of claim 36, wherein said radio link control layer of said wireless modem protocol stack comprises functionality for the transmission of one or more logical link control (LLC) frames of information on an over-the-air interface between said wireless modem and a base station.

48. The wireless access network of claim 36, wherein said medium access control layer of said wireless modem protocol stack comprises functionality for multiplexing two or more logical link control (LLC) frames of information on an uplink channel of an over-the-air interface between said wireless modem and a base station.

49. The wireless access network of claim 36, wherein said logical link control layer of said wireless modem protocol stack comprises functionality for

generating and transmitting one or more logical link control (LLC) frames of information from said wireless modem to a base station.

50. The wireless access network of claim 36, wherein said subnetwork dependent convergence protocol layer of said wireless modem protocol stack comprises functionality for mapping an Internet Protocol message to one or more logical link control frames, for transmission by said wireless modem on an over-the-air interface to a base station, and further comprises functionality for mapping one or more logical link control frames received by said wireless modem from a base station to an Internet Protocol message.

51. The wireless access network of claim 36 further comprising a base station and an access router, wherein said base station comprises a base station protocol stack, and said base station protocol stack comprises a frame relay layer for communicating with said access router.

52. The wireless access network of claim 51, wherein said frame relay layer of said base station protocol stack comprises functionality for mapping a switched virtual circuit address of a message transmitted from said access router to a temporary logical link identity address, for transmission of said message to said wireless modem.

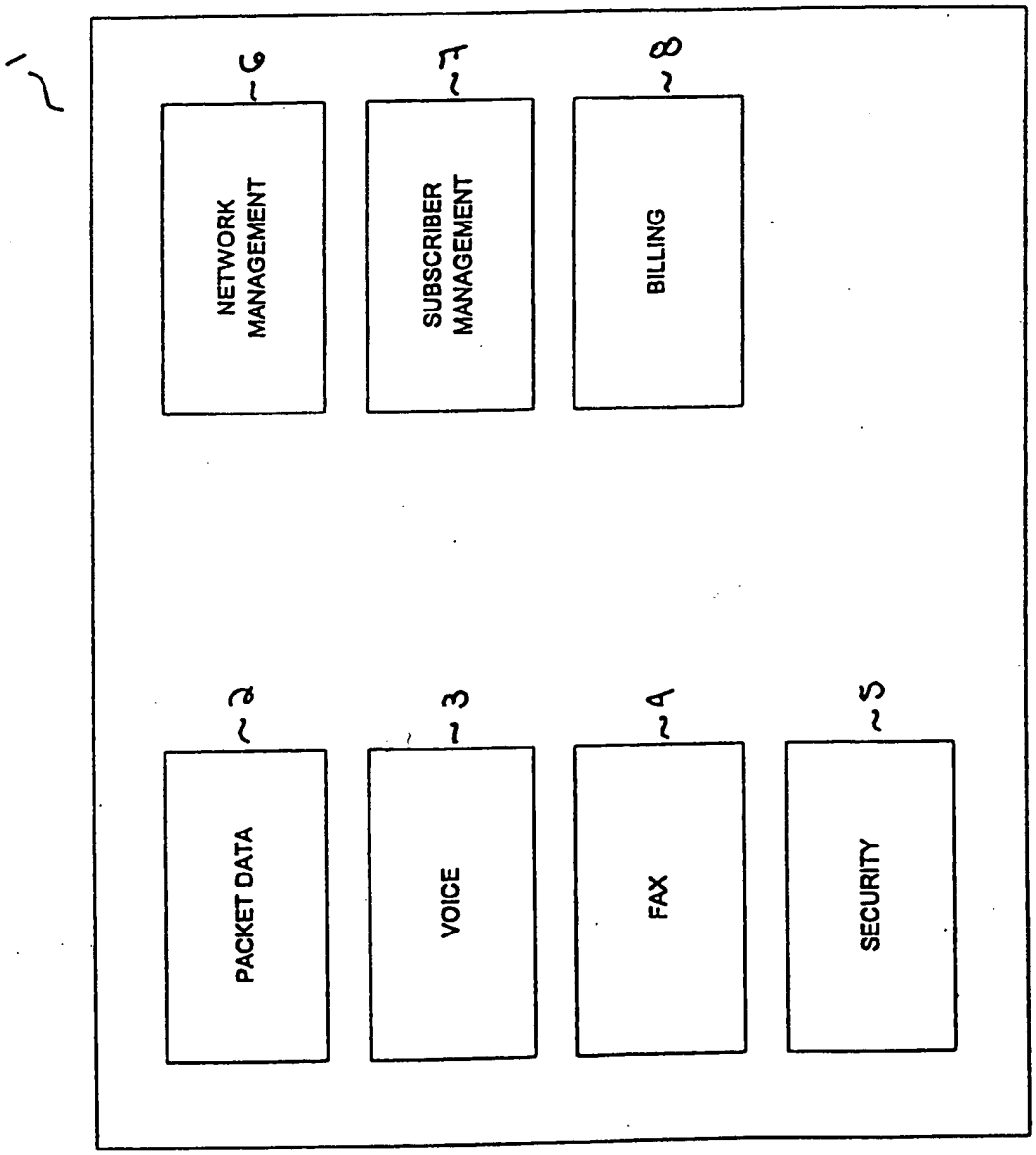

1
6
7
8
NETWORK MANAGEMENT
SUBSCRIBER MANAGEMENT
BILLING
2
3
4
5
PACKET DATA
VOICE
FAX
SECURITY

FIGURE 1

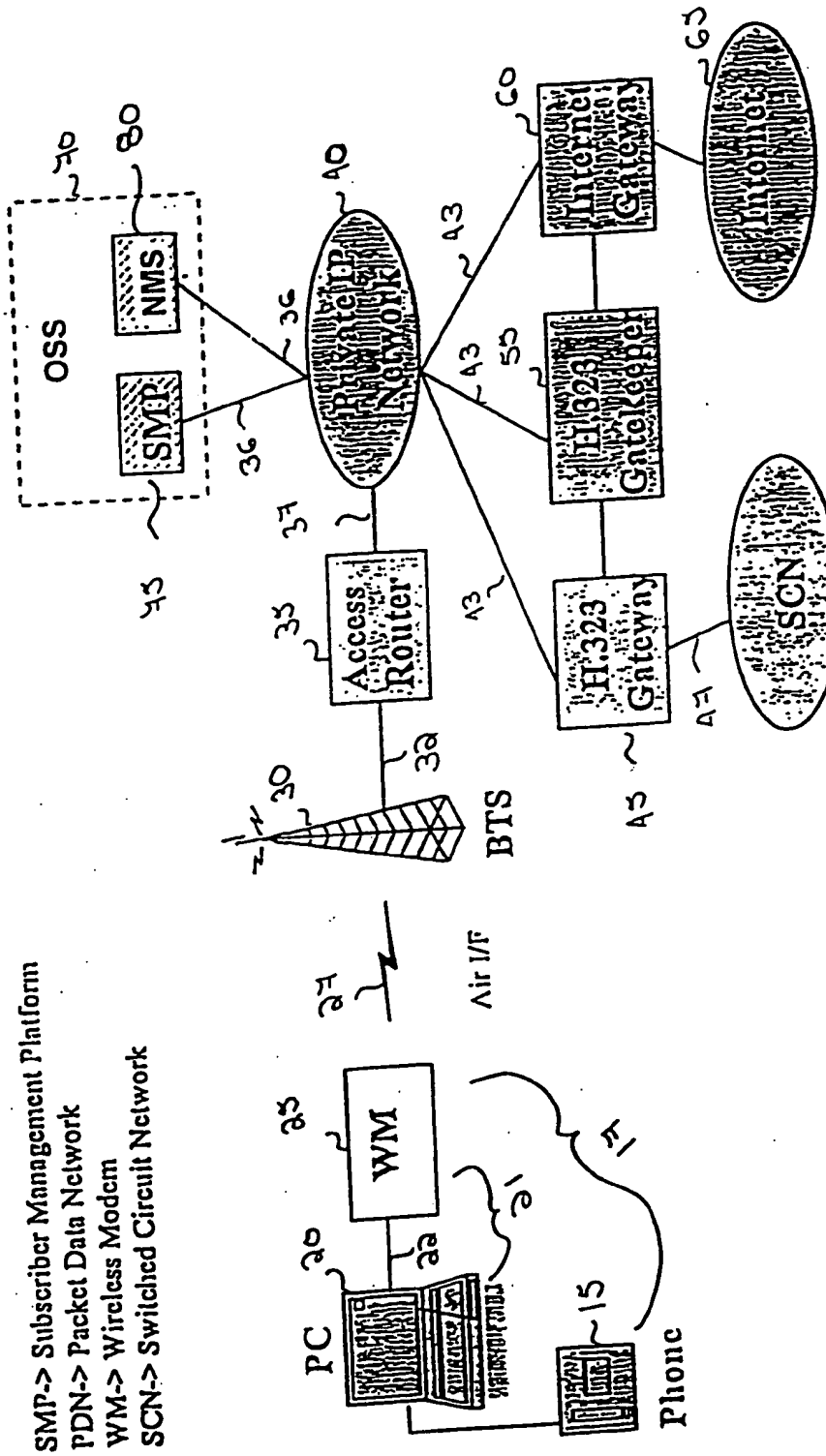

10
OSS
NMS
SMP
80
70
36
45
40
Packet Data Network
43
60
Internet Gateway
65
55
H.323 GateKeeper
35
Access Router
37
39
30
BTS
43
H.323 Gateway
47
SCN
50
Air I/F
25
WM
21
41
PC
20
23
15
Phone
SMP-> Subscriber Management Platform
PDN-> Packet Data Network
WM-> Wireless Modem
SCN-> Switched Circuit Network

FIGURE 2

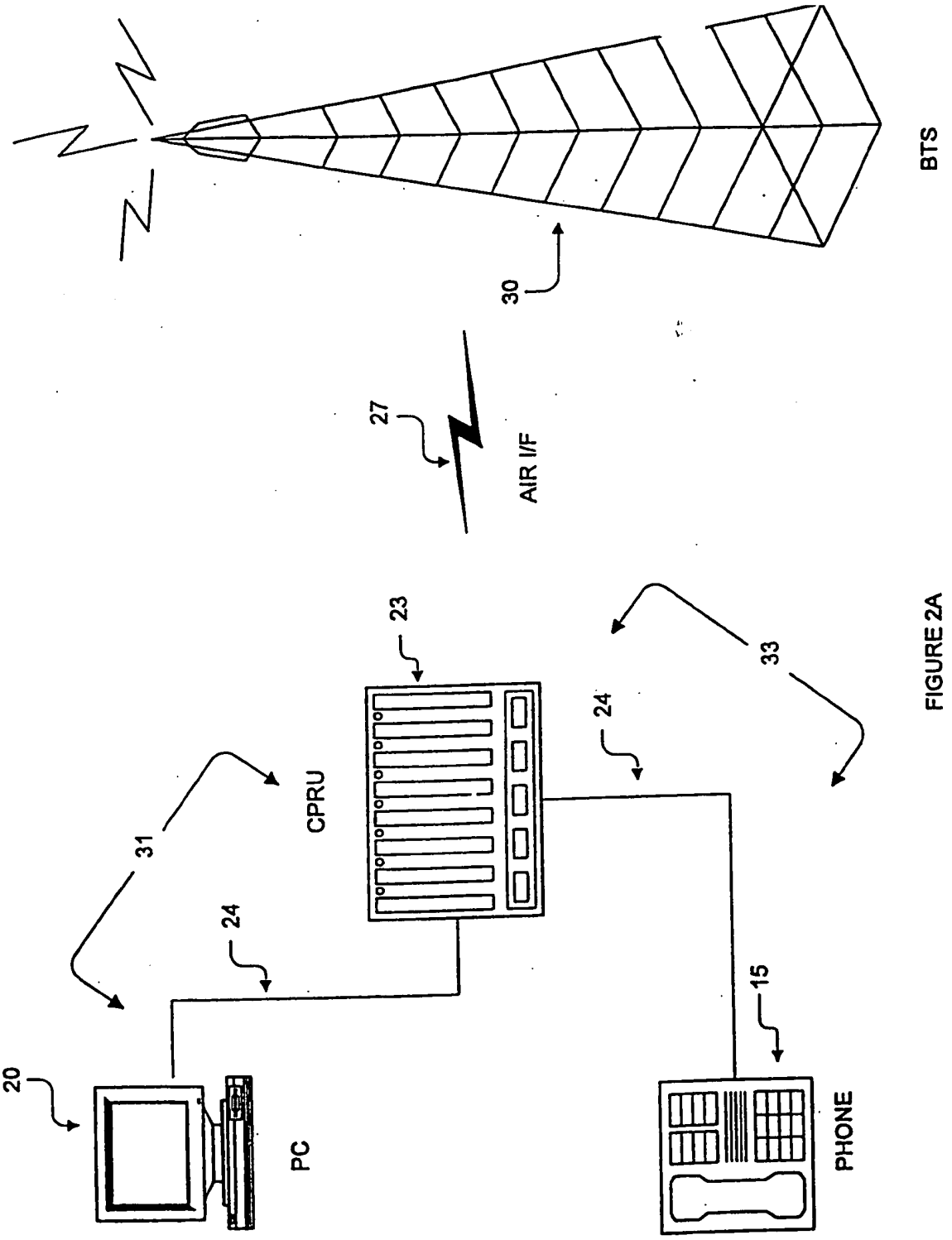


FIGURE 2A

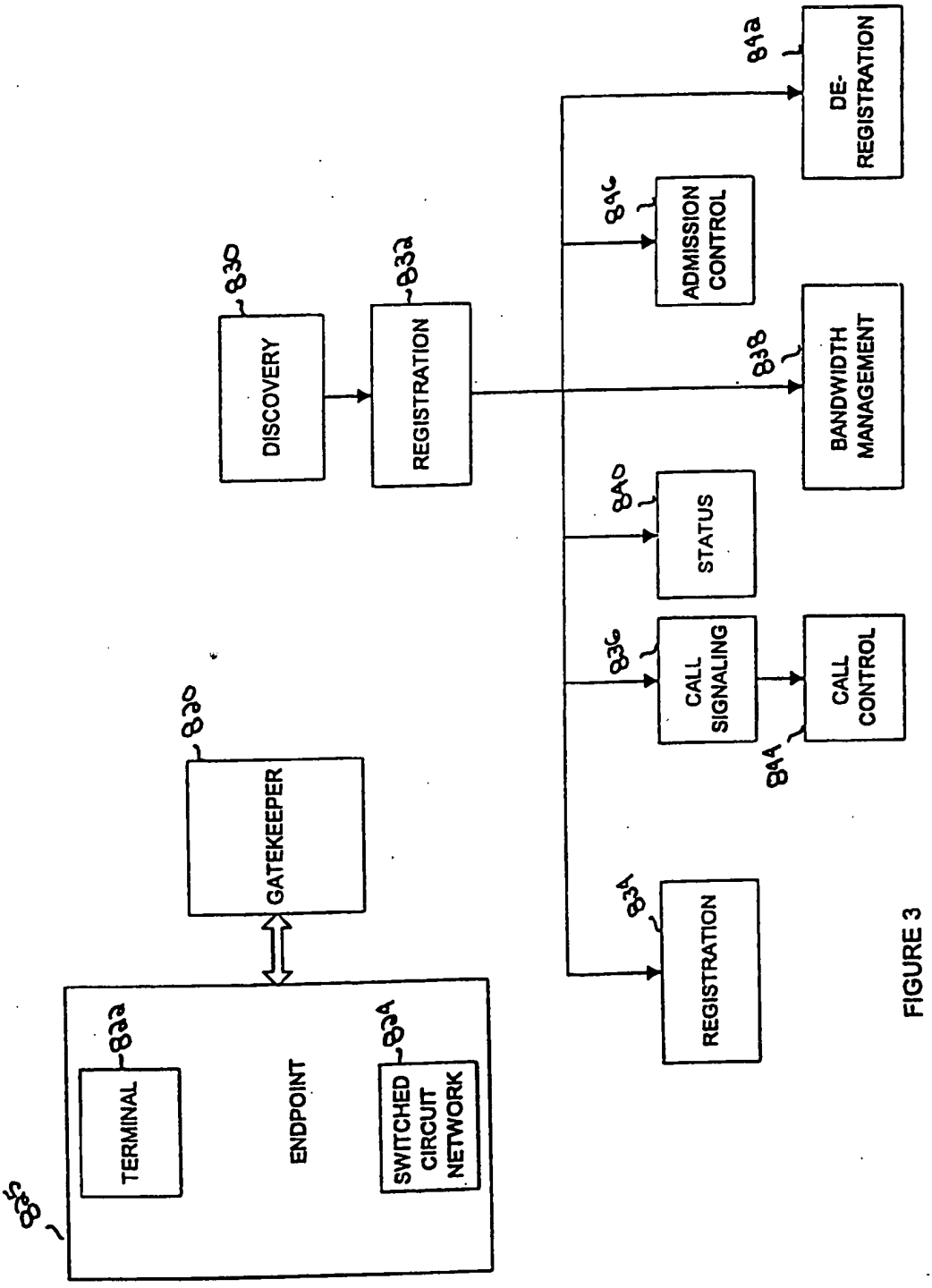

DE-REGISTRATION
ADMISSION CONTROL
BANDWIDTH MANAGEMENT
STATUS
CALL SIGNALING
CALL CONTROL
REGISTRATION
DISCOVERY
REGISTRATION
GATEKEEPER
TERMINAL
ENDPOINT
SWITCHED CIRCUIT NETWORK

FIGURE 3

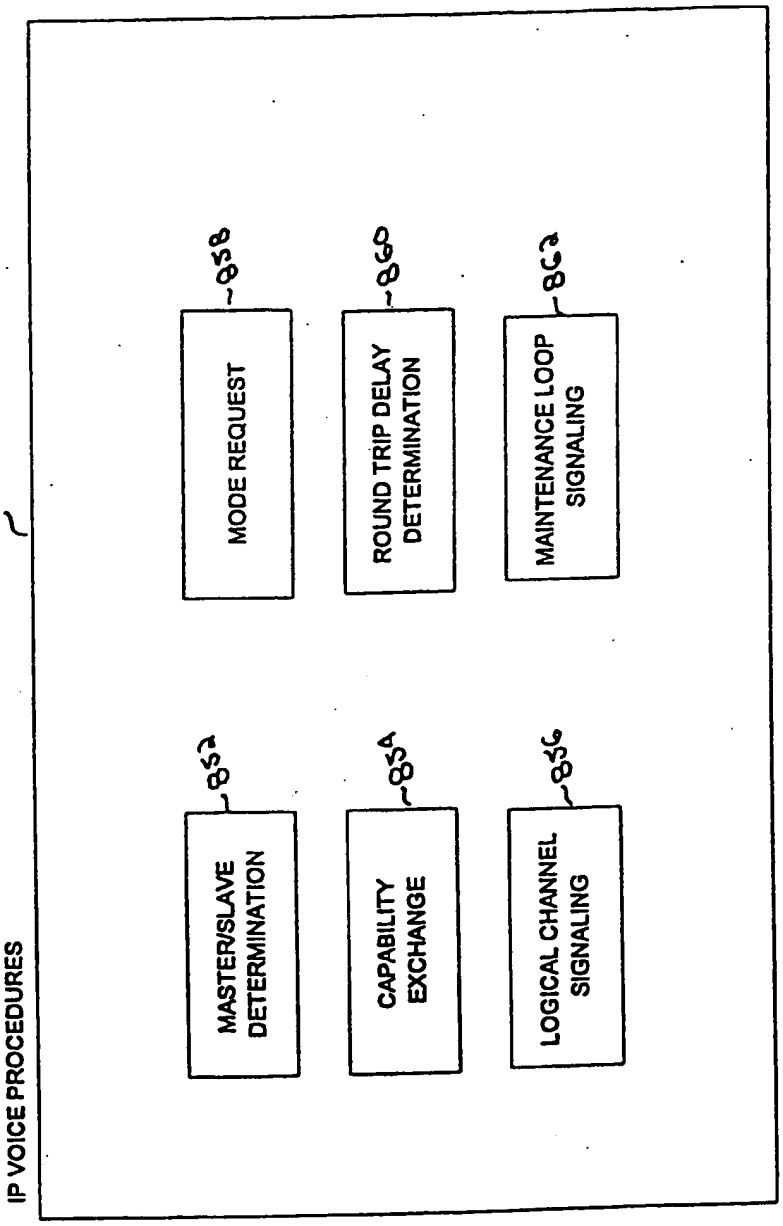

848
IP VOICE PROCEDURES
MASTER/SLAVE DETERMINATION
852
CAPABILITY EXCHANGE
854
LOGICAL CHANNEL SIGNALING
856
MODE REQUEST
858
ROUND TRIP DELAY DETERMINATION
860
MAINTENANCE LOOP SIGNALING
862

FIGURE 4

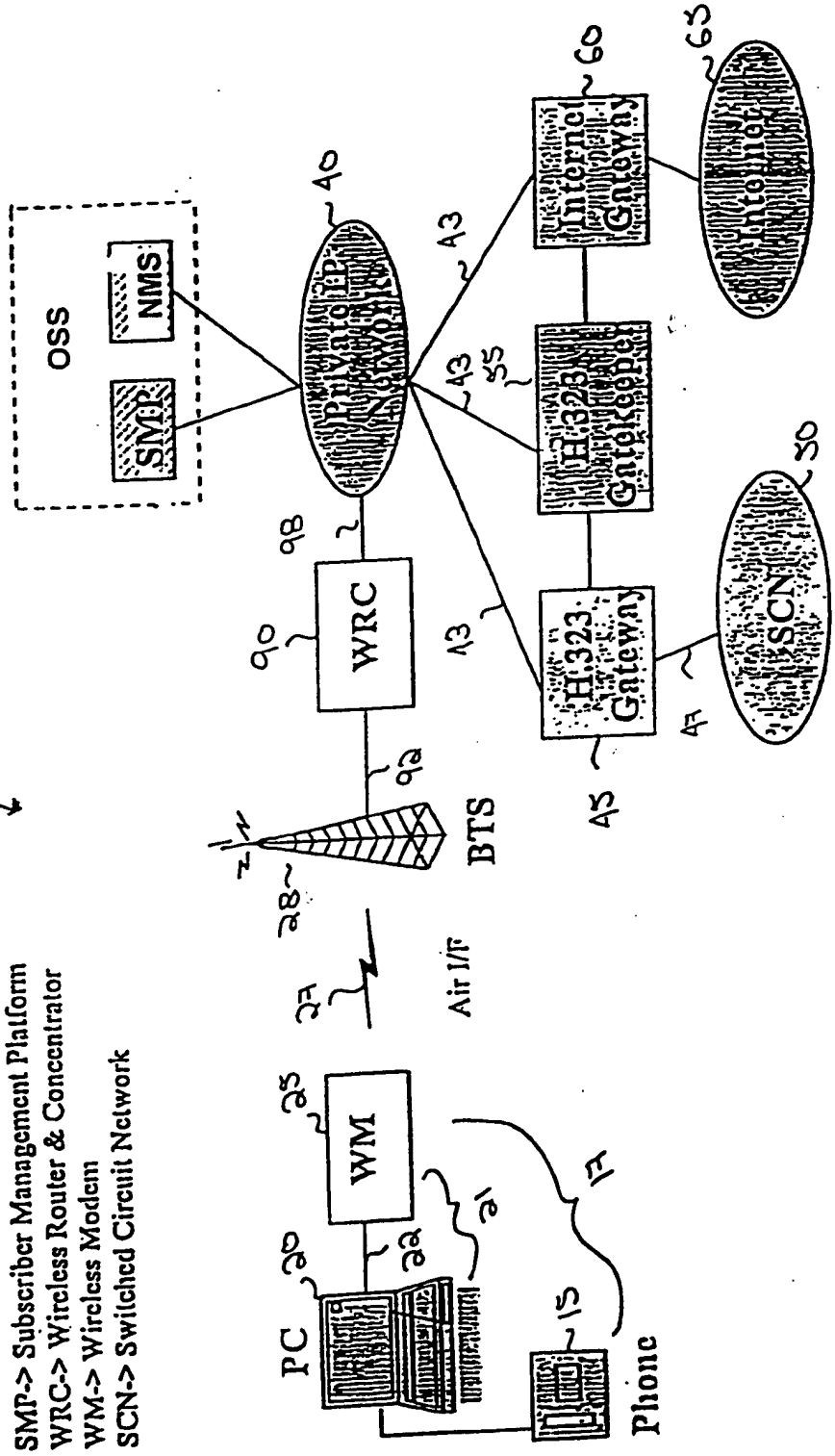

OSS
NMS
SMP
Private IP Network
40
43
Internet Gateway
60
63
H.323 Gateway
55
43
PSTN
50
WRC
90
98
43
H.323 Gateway
45
47
100
BTS
Air I/F
WM
95
PC
20
Phone
15
11
SMP-> Subscriber Management Platform
WRC-> Wireless Router & Concentrator
WM-> Wireless Modem
SCN-> Switched Circuit Network

FIGURE 5

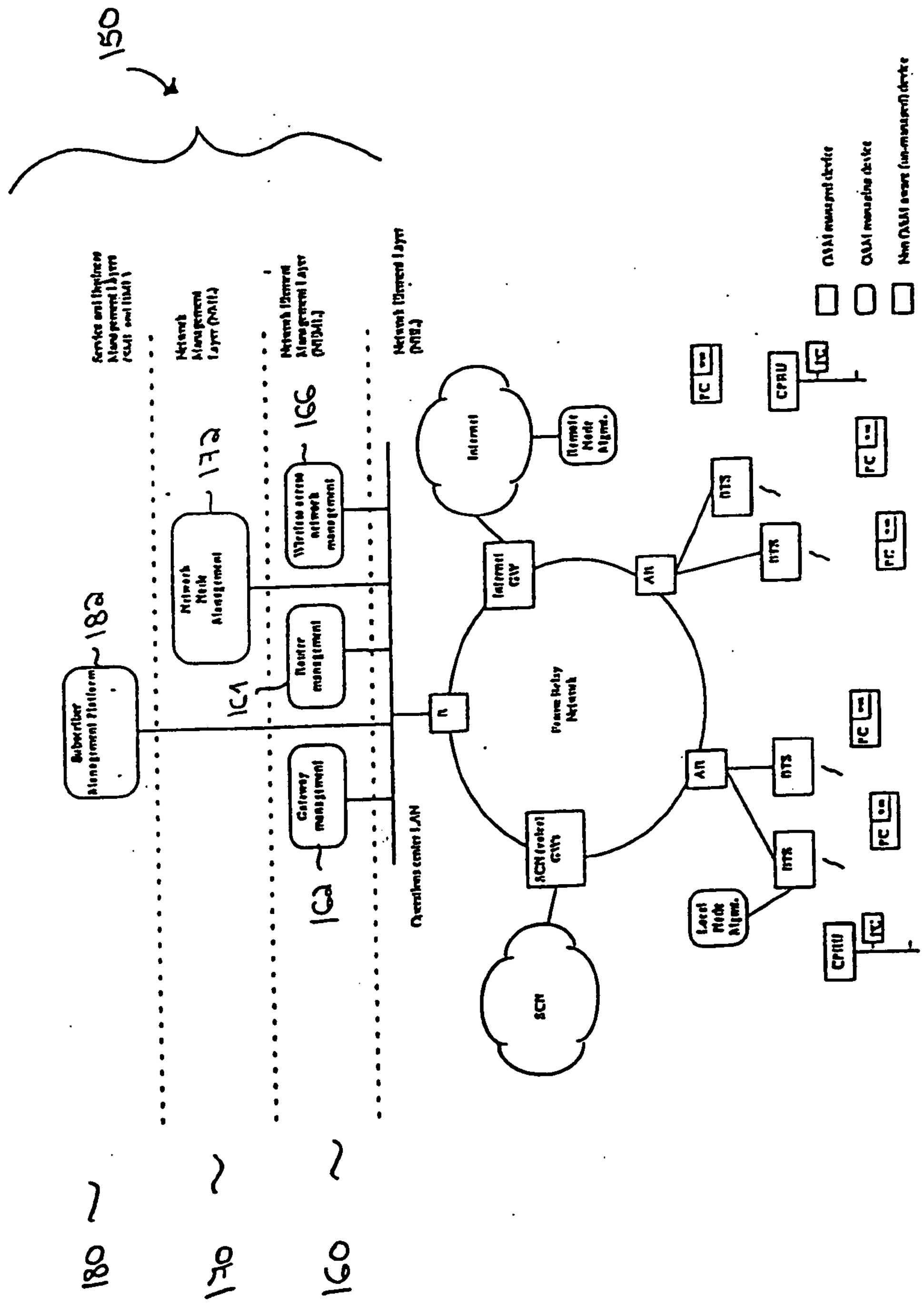


FIGURE 6

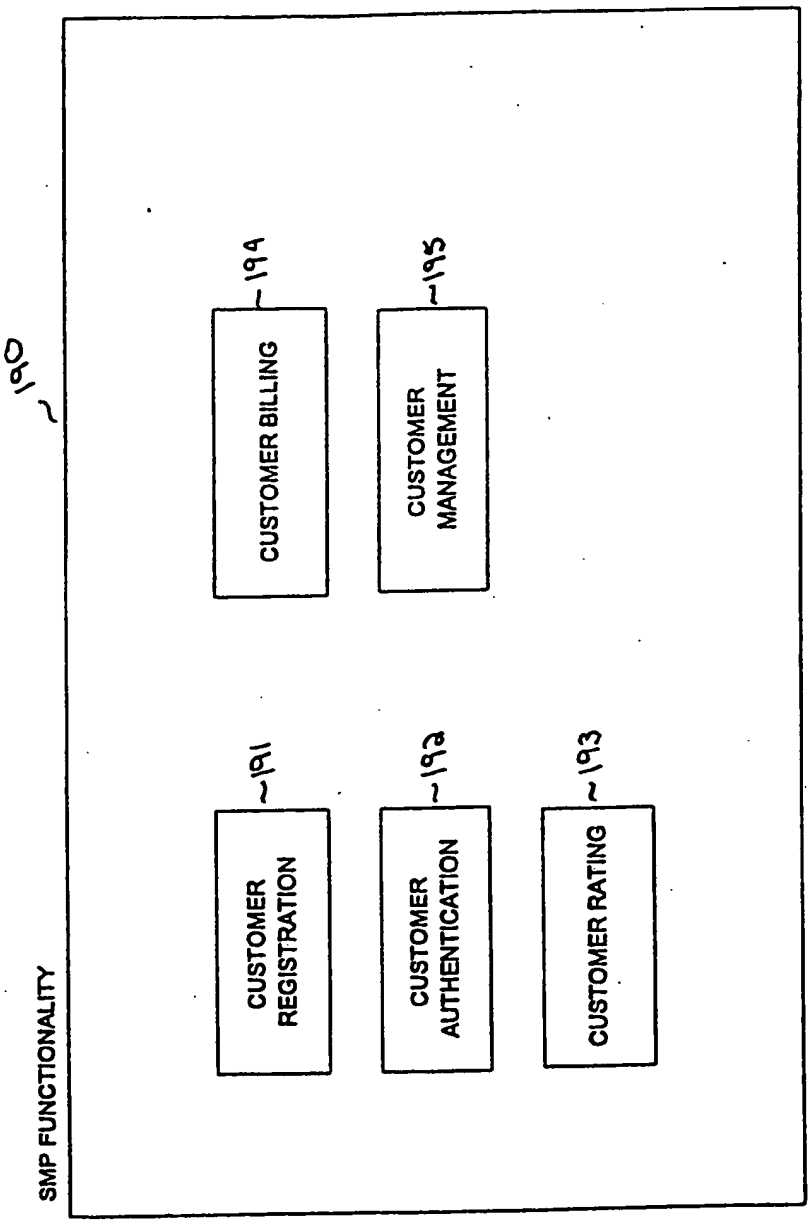

190
SMP FUNCTIONALITY
CUSTOMER REGISTRATION
191
CUSTOMER AUTHENTICATION
192
CUSTOMER RATING
193
CUSTOMER BILLING
194
CUSTOMER MANAGEMENT
195

FIGURE 7

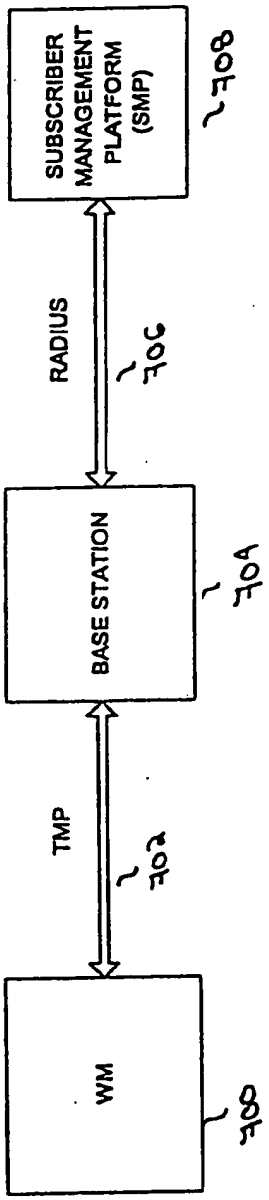

SUBSCRIBER MANAGEMENT PLATFORM (SMP)
708
RADIUS
706
BASE STATION
704
TMP
702
WM
700

FIGURE 8

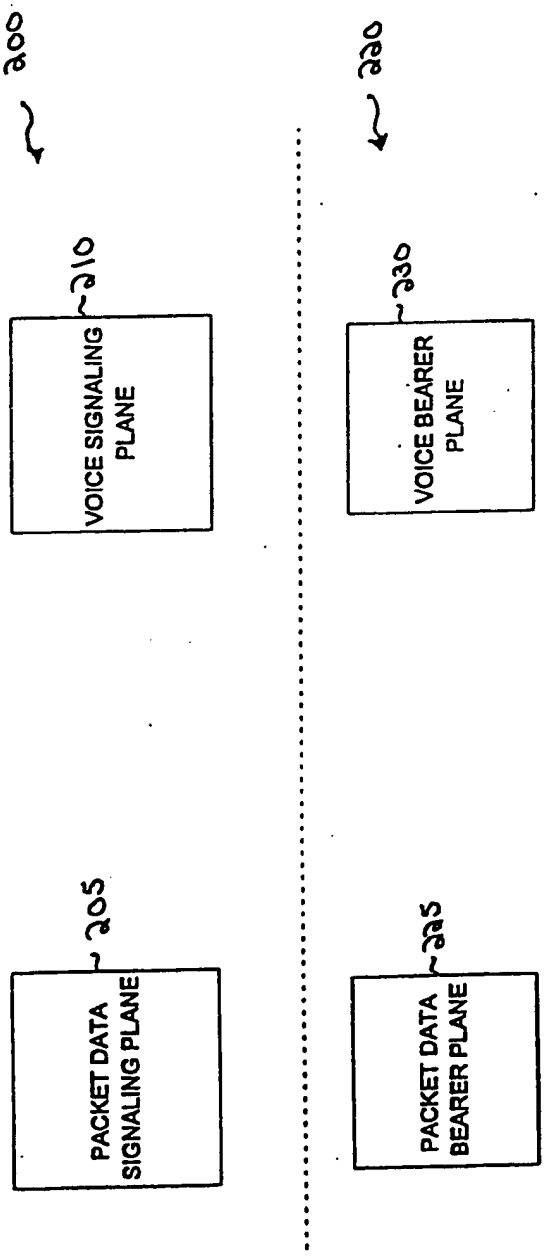

200
220
210
VOICE SIGNALING PLANE
230
VOICE BEARER PLANE
205
PACKET DATA SIGNALING PLANE
225
PACKET DATA BEARER PLANE

FIGURE 9

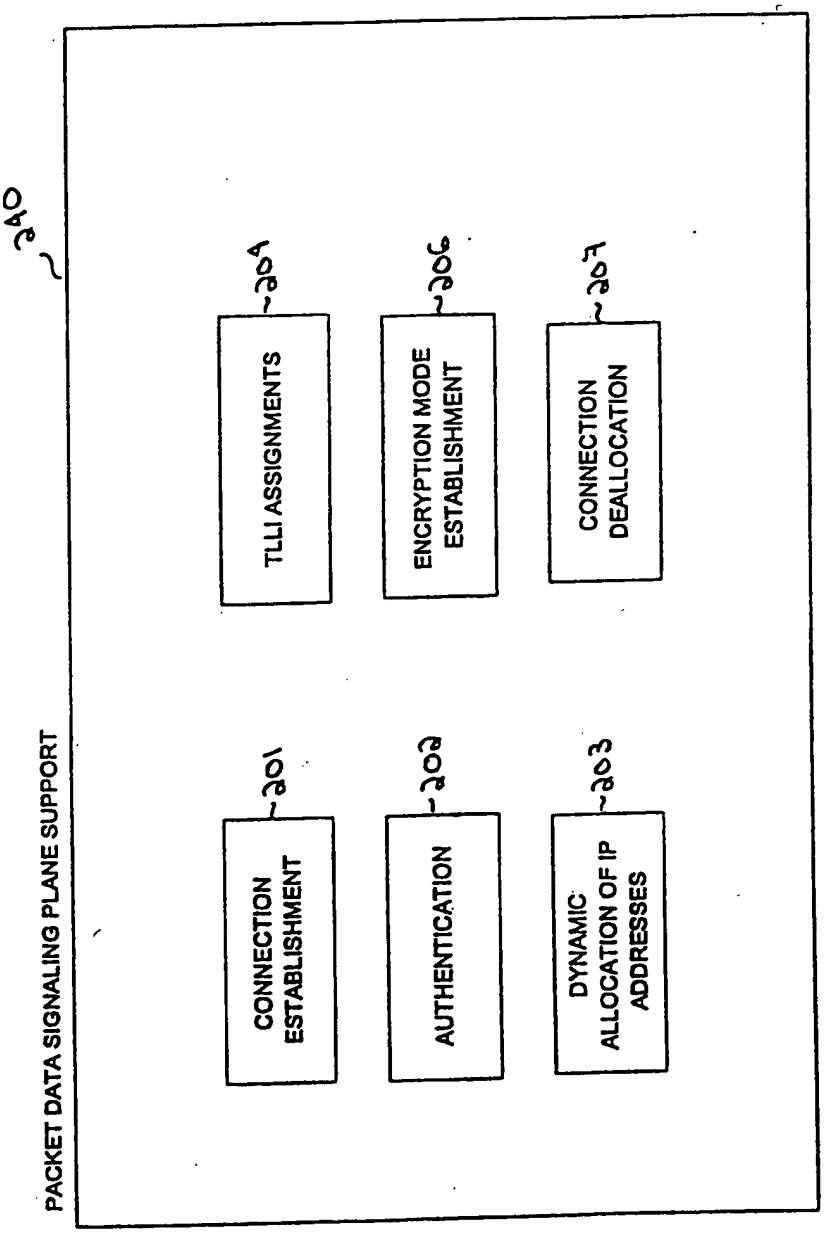

240
PACKET DATA SIGNALING PLANE SUPPORT
201
CONNECTION ESTABLISHMENT
202
AUTHENTICATION
203
DYNAMIC ALLOCATION OF IP ADDRESSES
204
TLLI ASSIGNMENTS
206
ENCRYPTION MODE ESTABLISHMENT
207
CONNECTION DEALLOCATION

FIGURE 10

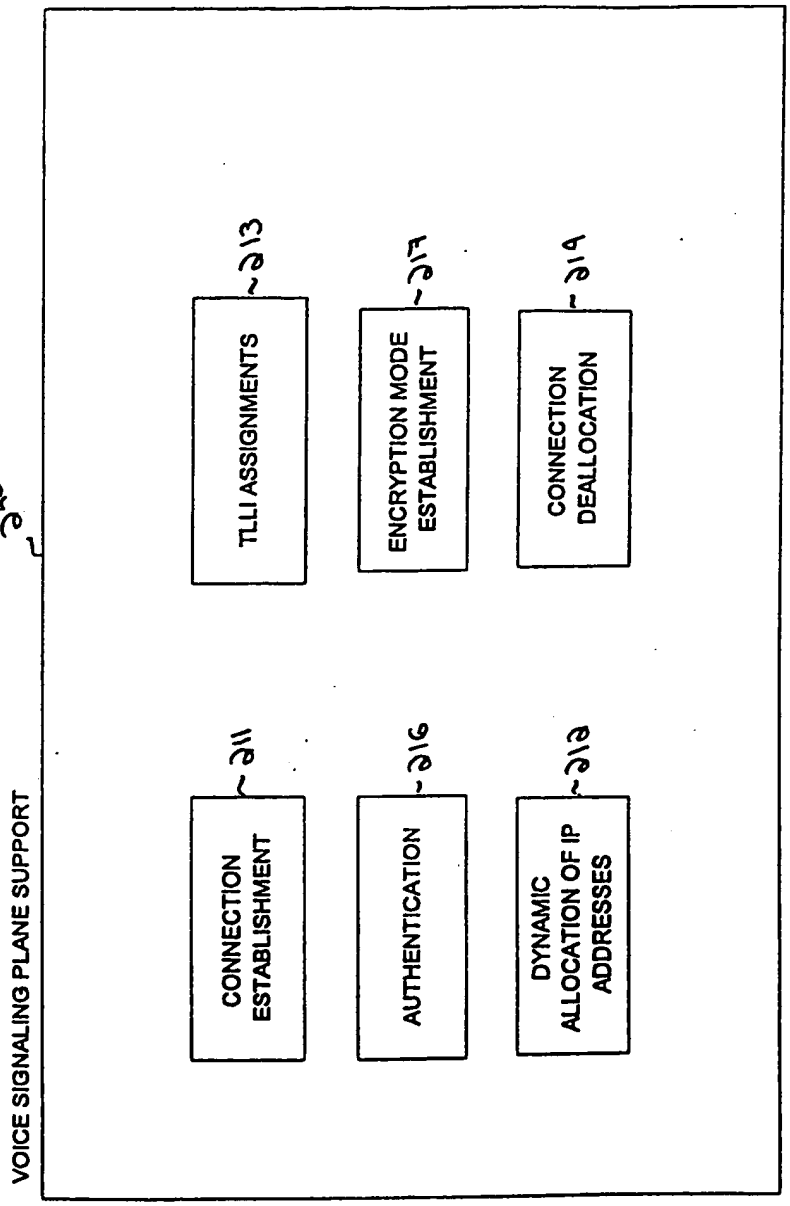

VOICE SIGNALING PLANE SUPPORT
315
TLLI ASSIGNMENTS
313
ENCRYPTION MODE ESTABLISHMENT
317
CONNECTION DEALLOCATION
319
CONNECTION ESTABLISHMENT
311
AUTHENTICATION
316
DYNAMIC ALLOCATION OF IP ADDRESSES
318

FIGURE 11

BEST AVAILABLE COPY

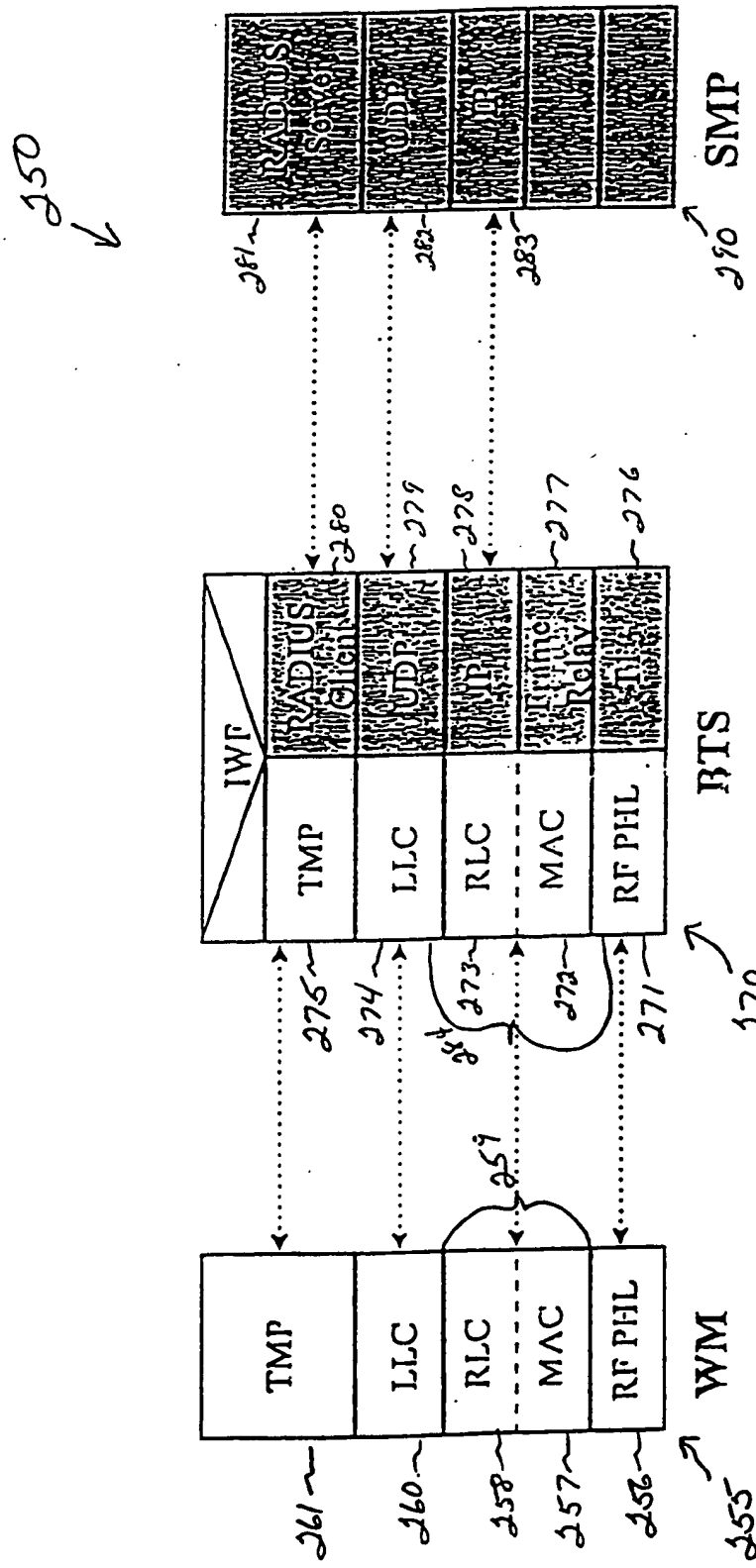


FIGURE 12

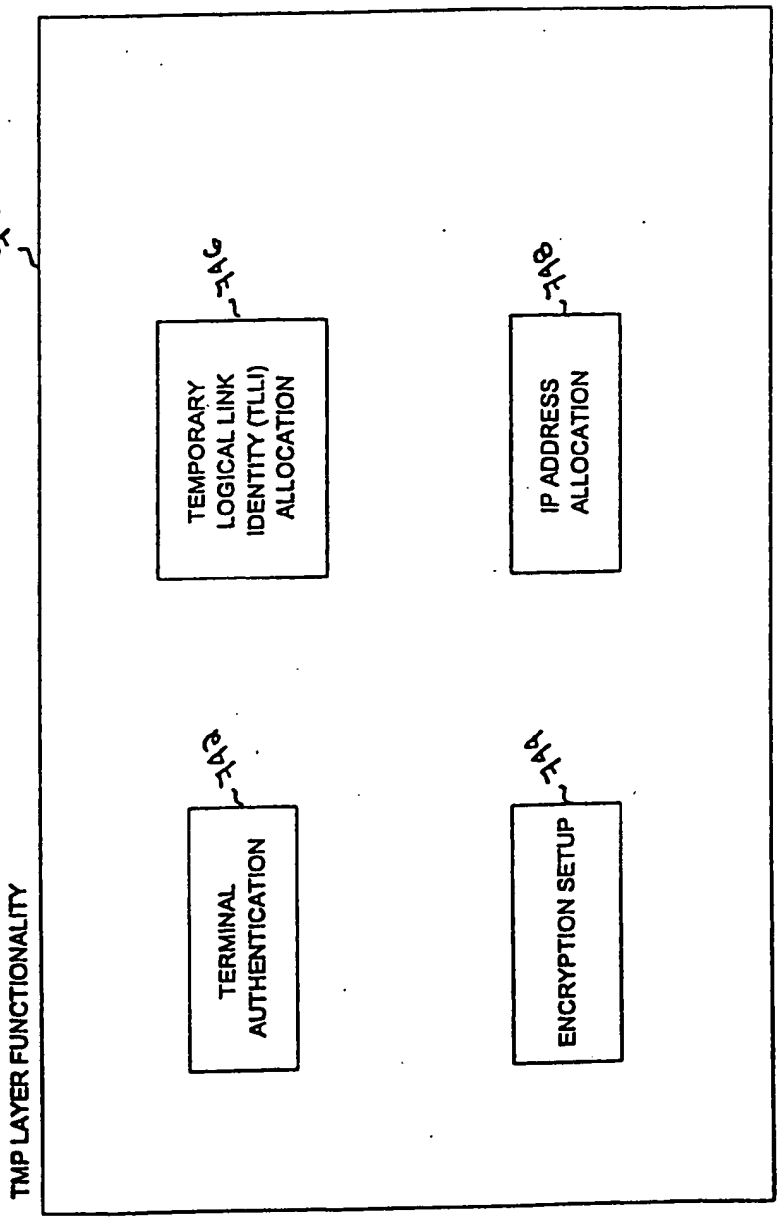

TMP LAYER FUNCTIONALITY
TERMINAL AUTHENTICATION
ENCRYPTION SETUP
TEMPORARY LOGICAL LINK IDENTITY (TLLI) ALLOCATION
IP ADDRESS ALLOCATION

FIGURE 13

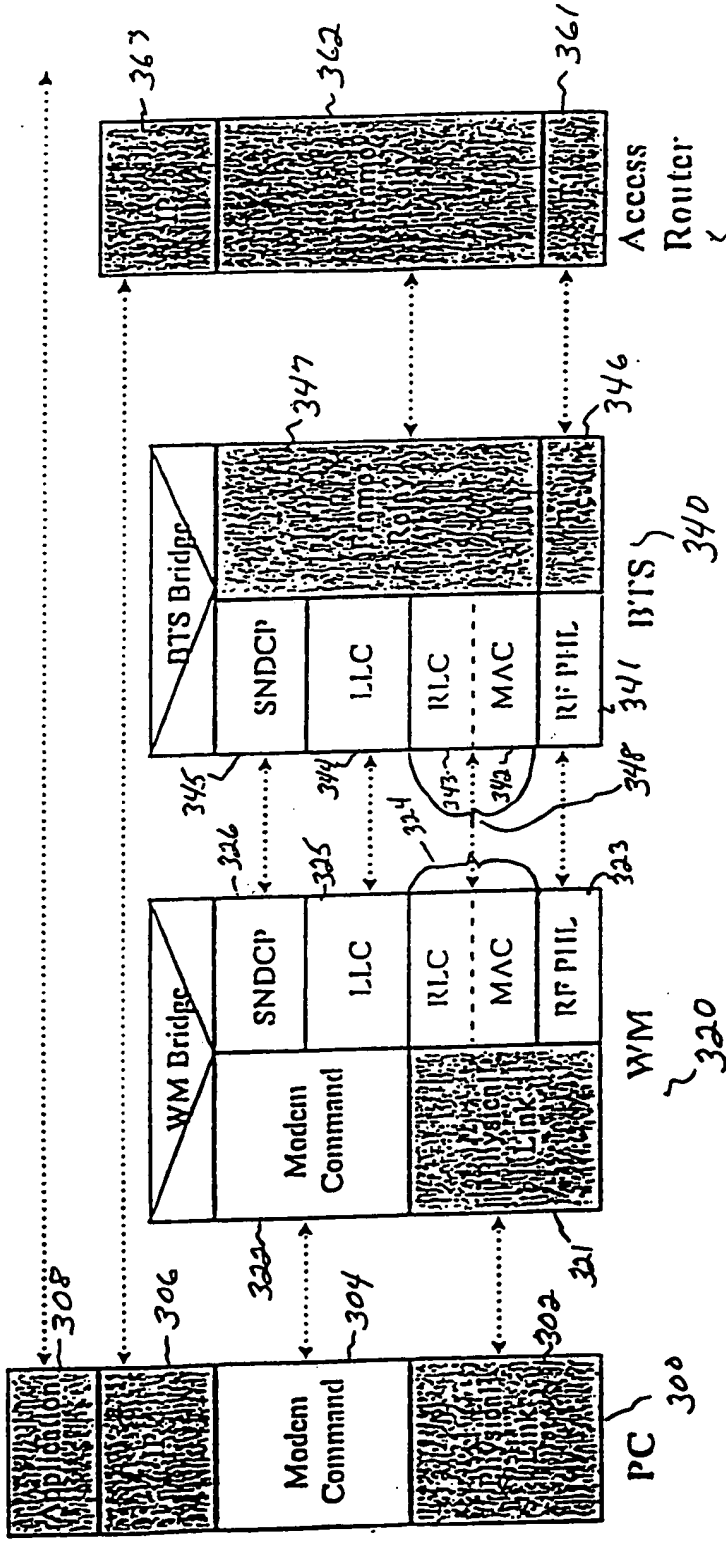


FIGURE 14

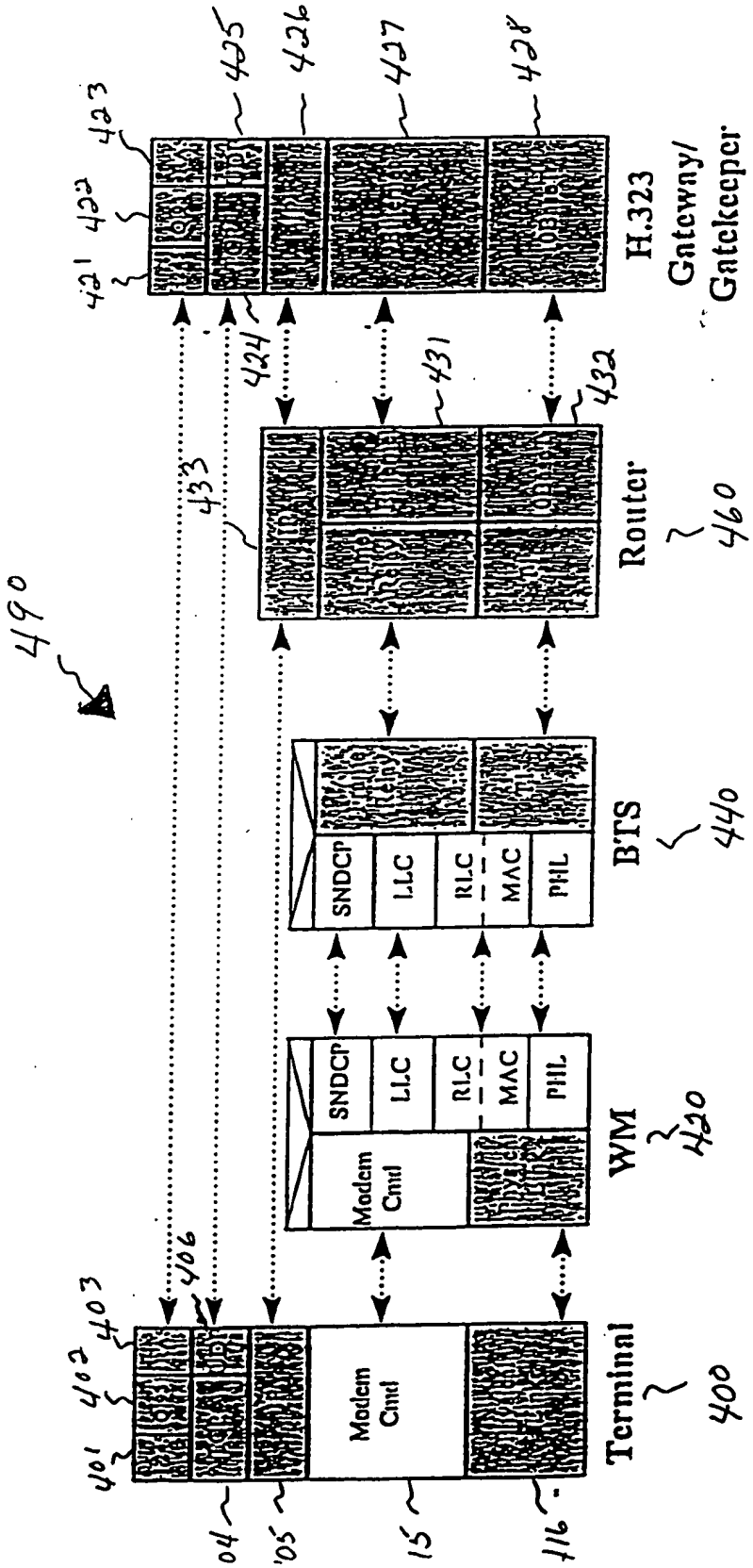


FIGURE 15

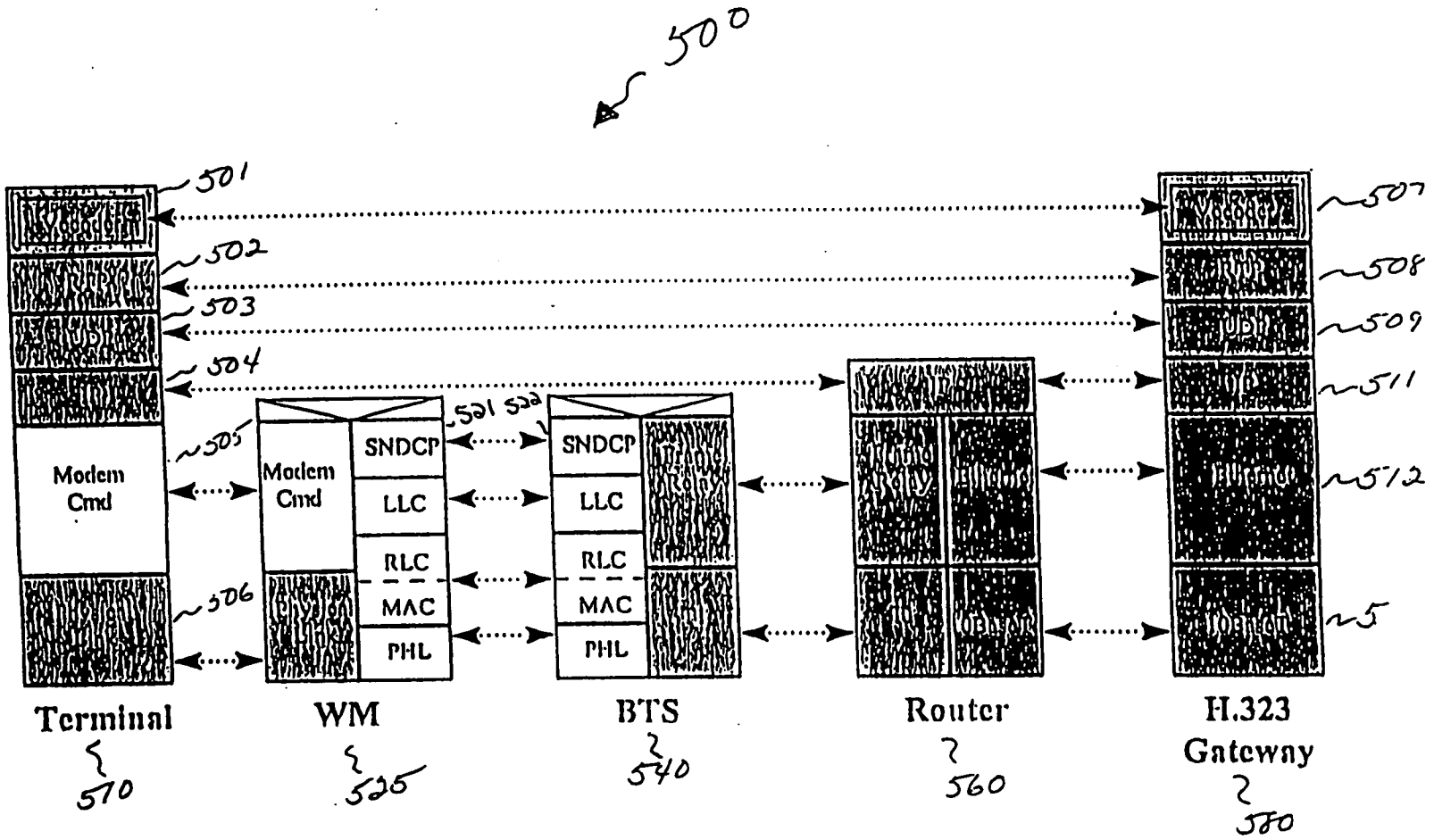


FIGURE 16

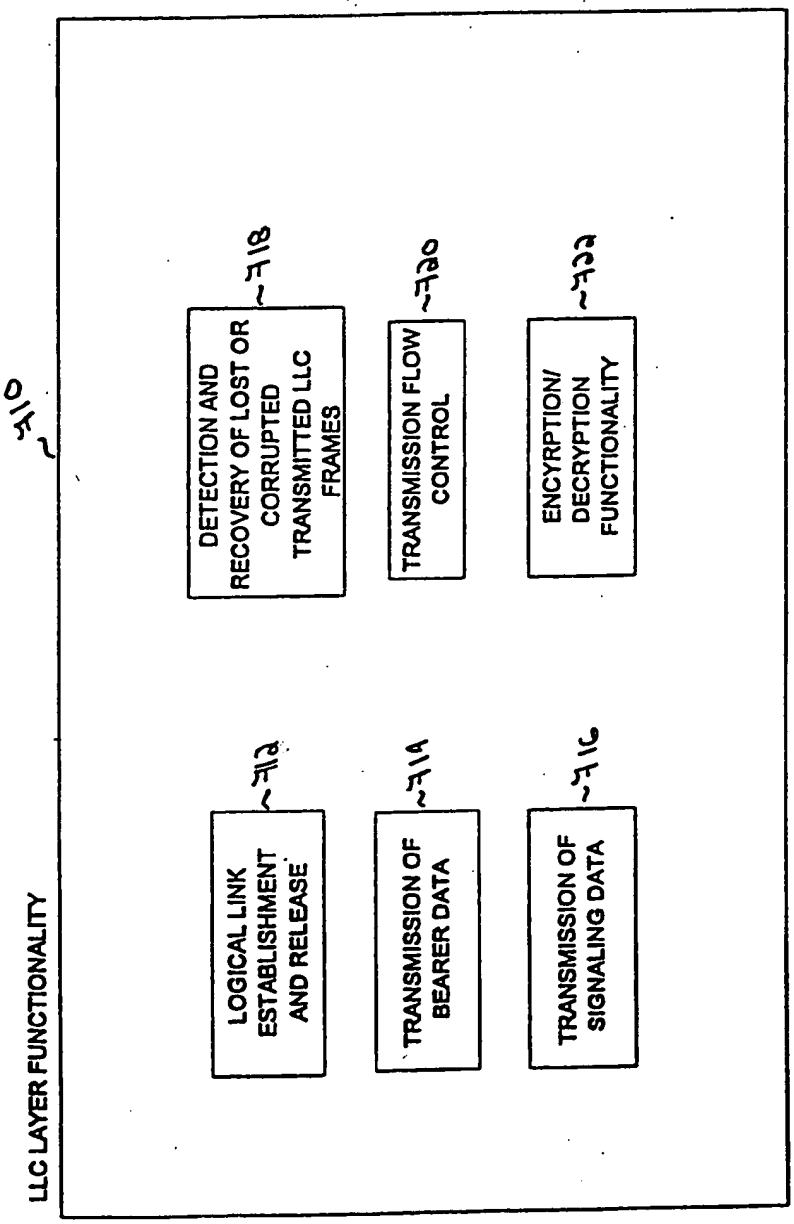

LLC LAYER FUNCTIONALITY
310
DETECTION AND RECOVERY OF LOST OR CORRUPTED TRANSMITTED LLC FRAMES
318
TRANSMISSION FLOW CONTROL
320
ENCYRPTION/ DECRYPTION FUNCTIONALITY
322
LOGICAL LINK ESTABLISHMENT AND RELEASE
312
TRANSMISSION OF BEARER DATA
314
TRANSMISSION OF SIGNALING DATA
316

FIGURE 17

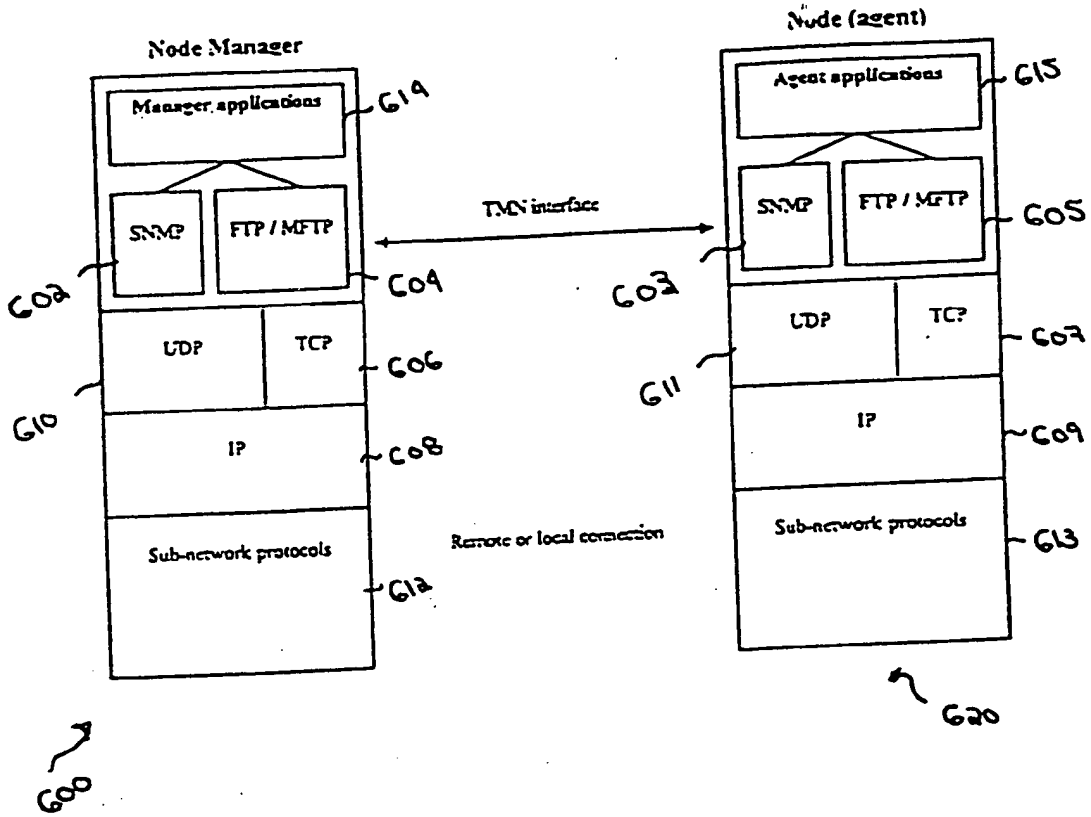

Node Manager
Manager applications
SNMP
FTP / MFTP
UDP
TCP
IP
Sub-network protocols
TMN interface
Remote or local connection
Node (agent)
Agent applications
SNMP
FTP / MFTP
UDP
TCP
IP
Sub-network protocols
600
602
603
604
605
606
607
608
609
610
611
612
613
614
615
620

FIGURE 18

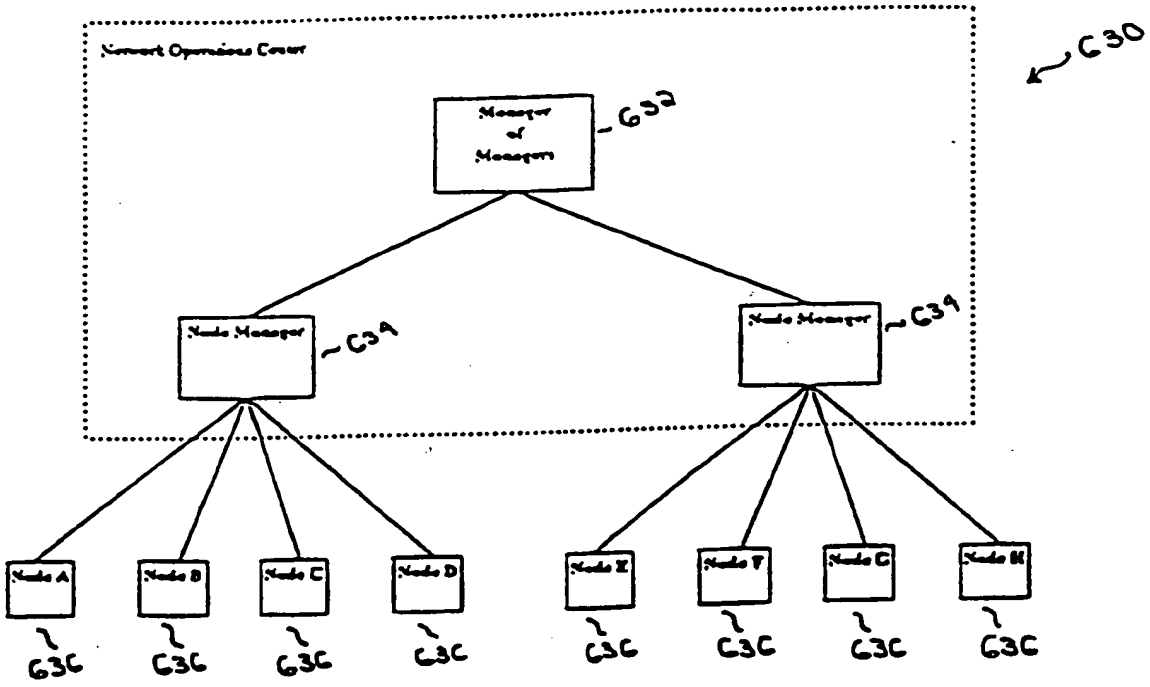

C30
Manager of Managers
632
Node Manager
634
Node Manager
634
Node A
Node B
Node C
Node D
Node E
Node F
Node G
Node H
636

FIGURE 19

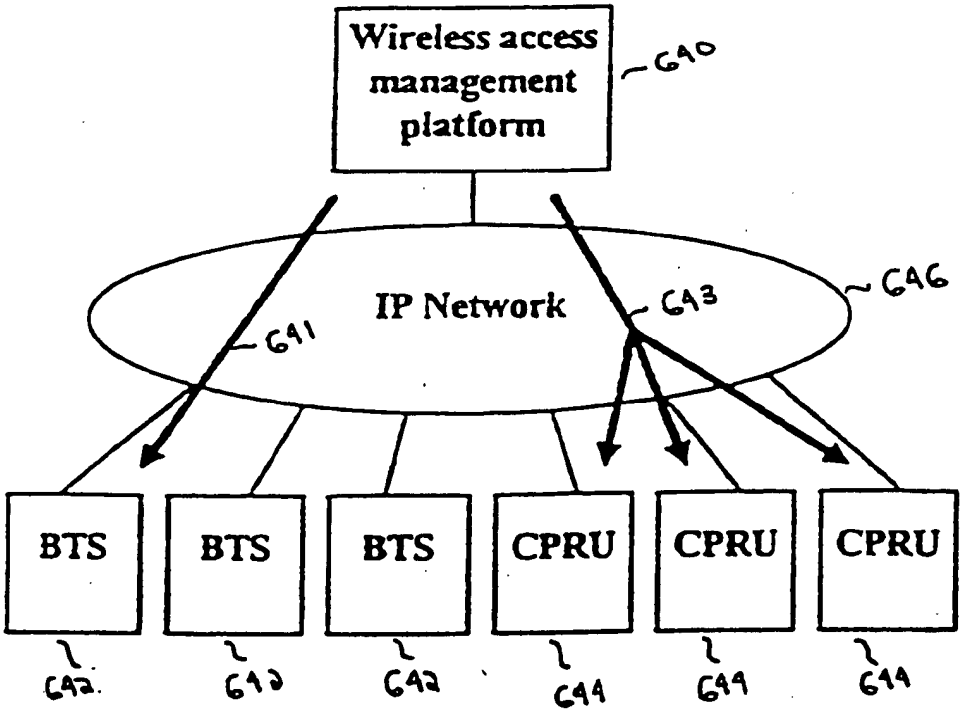

Wireless access management platform
640
IP Network
646
641
643
BTS
BTS
BTS
CPRU
CPRU
CPRU
642
642
642
644
649
649

FIGURE 20

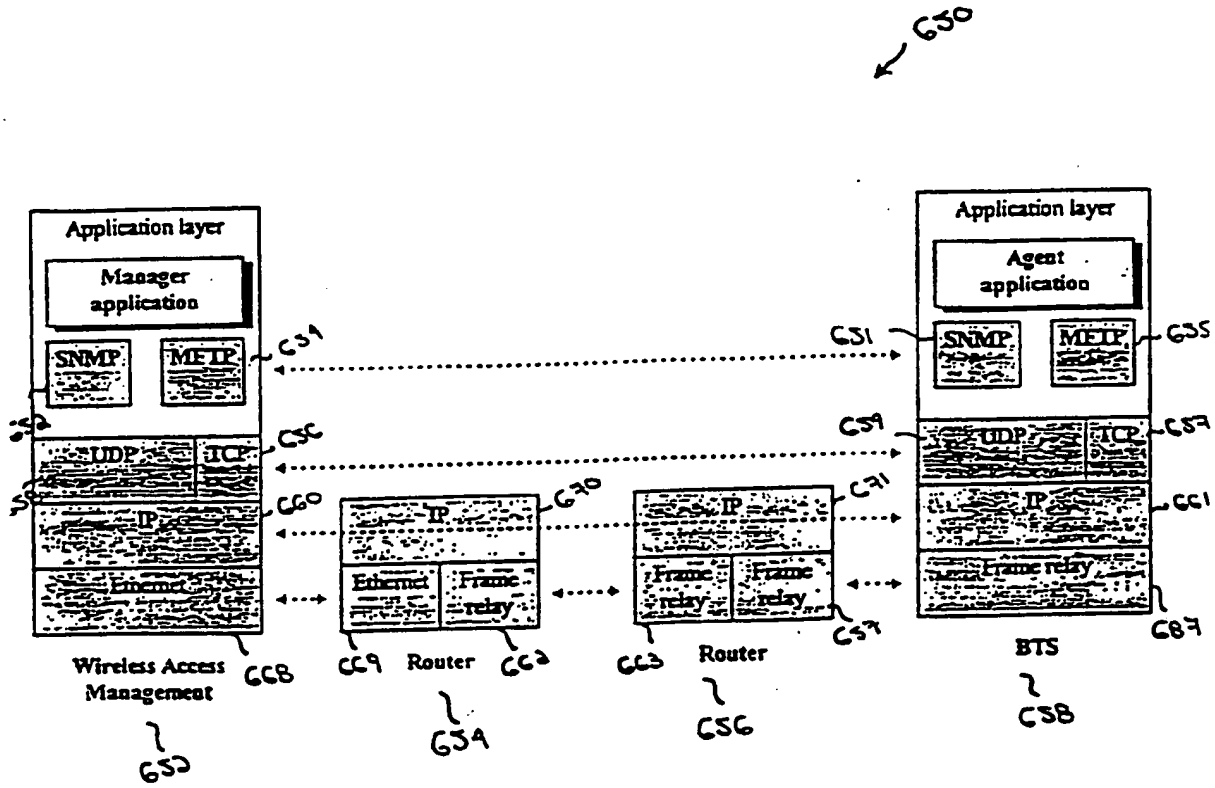

650
Application layer
Manager application
SNMP
MEIP
UDP
TCP
IP
Ethernet
Wireless Access Management
652
Router
IP
Ethernet
Frame relay
654
Router
IP
Frame relay
Frame relay
656
Application layer
Agent application
SNMP
MEIP
UDP
TCP
IP
Frame relay
BTS
658

FIGURE 21A

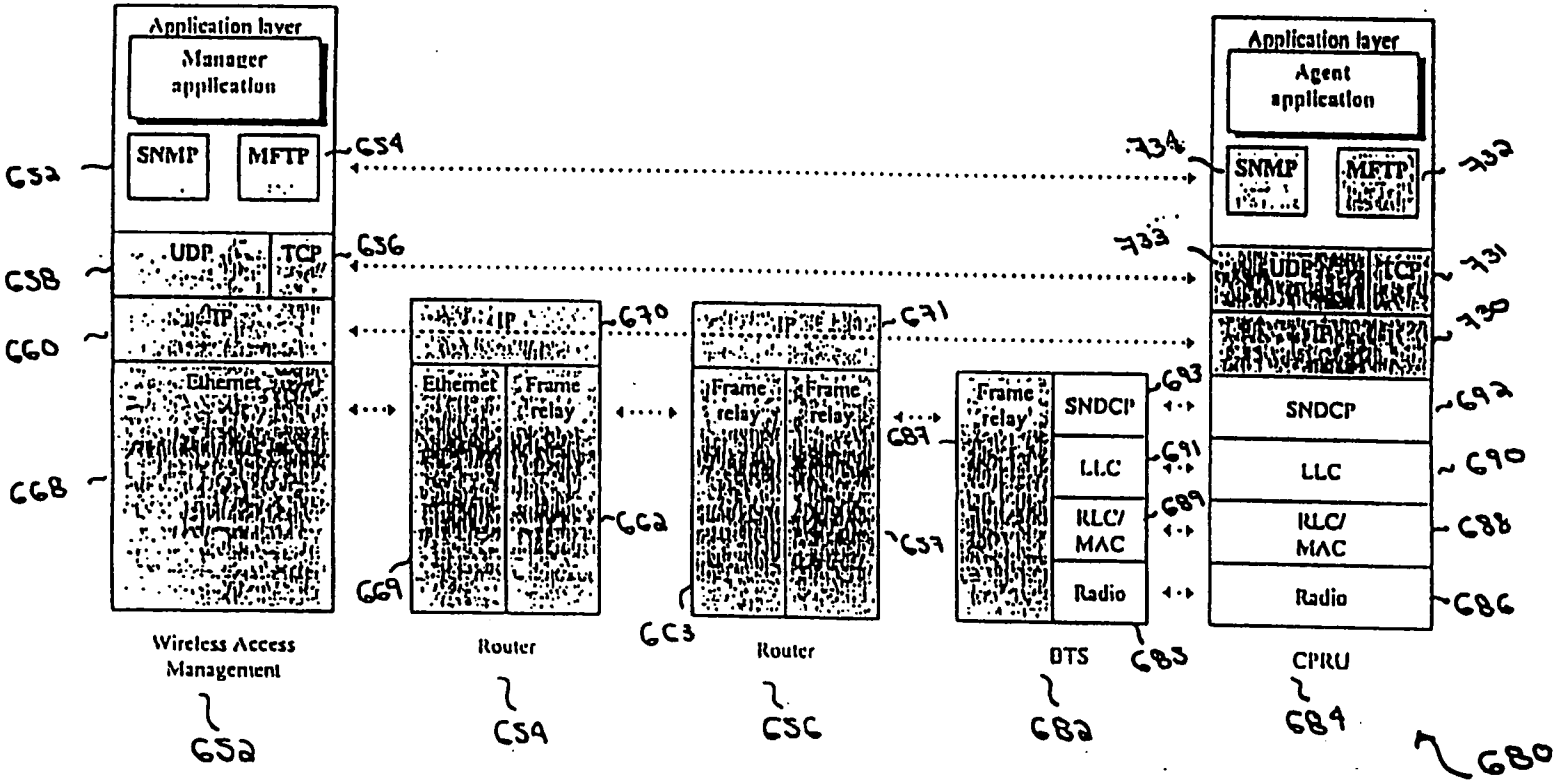


FIGURE 21B

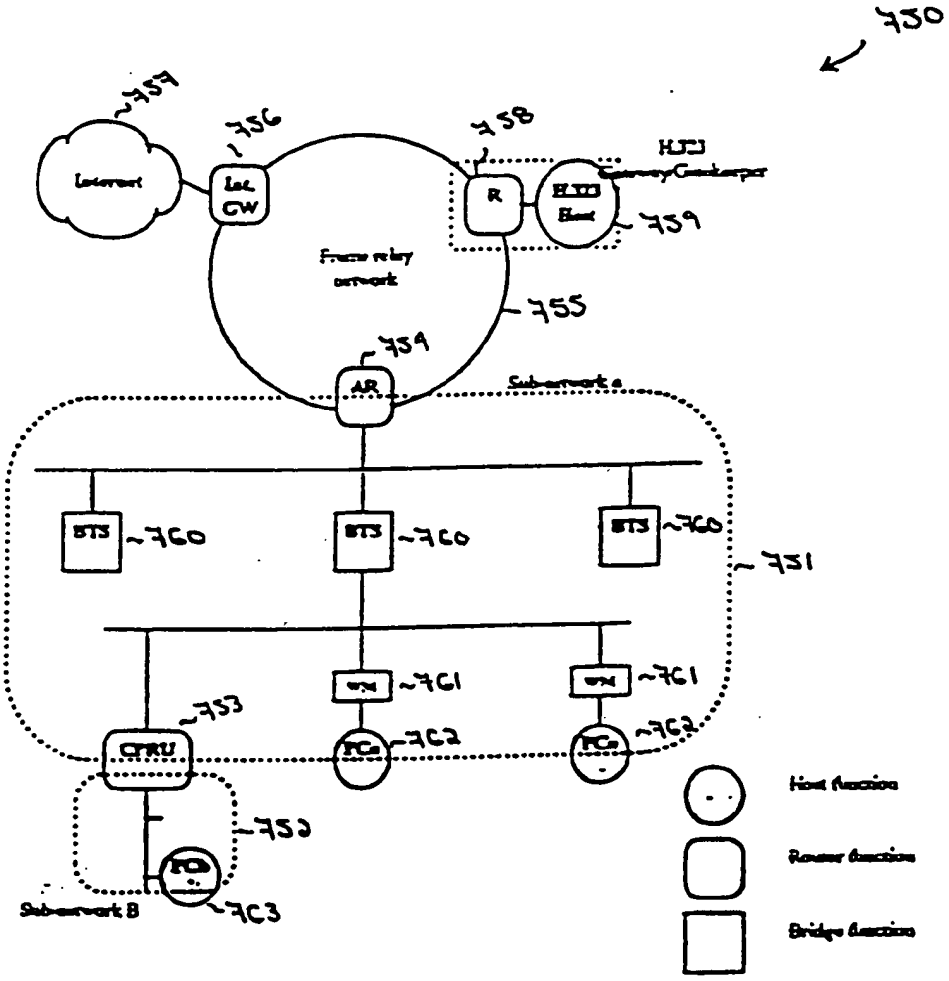

730
757
756
758
Internet
Int. GW
R
759
Frame relay network
755
759
AR
Subnetwork A
BTS
760
760
760
751
761
761
753
762
762
752
Subnetwork B
763
Host function
Router function
Bridge function

FIGURE 22

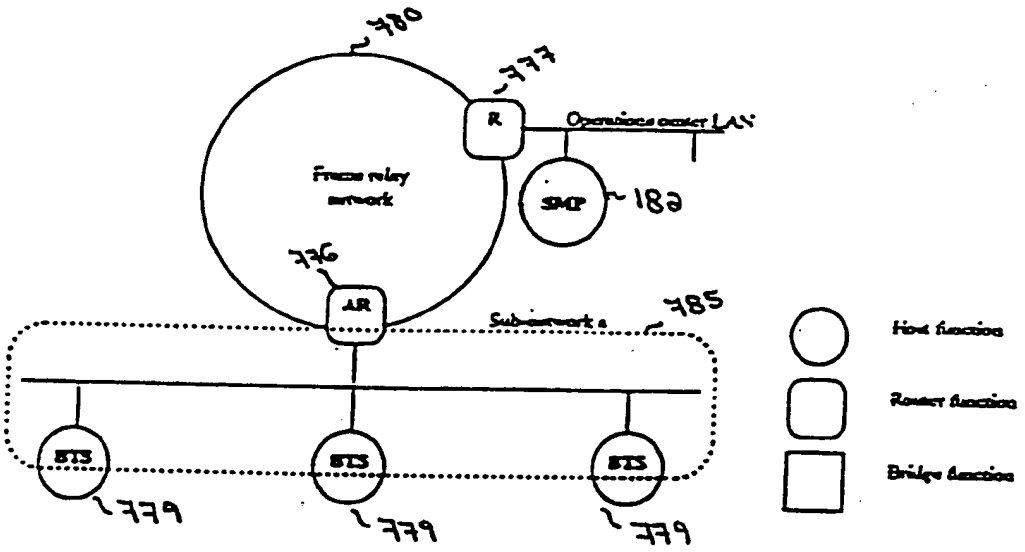

780
777
R
Operations center LAN
Frame relay network
SNCP
183
776
AR
Subnetwork a
785
STS
STS
STS
779
779
779
Host function
Router function
Bridge function

FIGURE 23

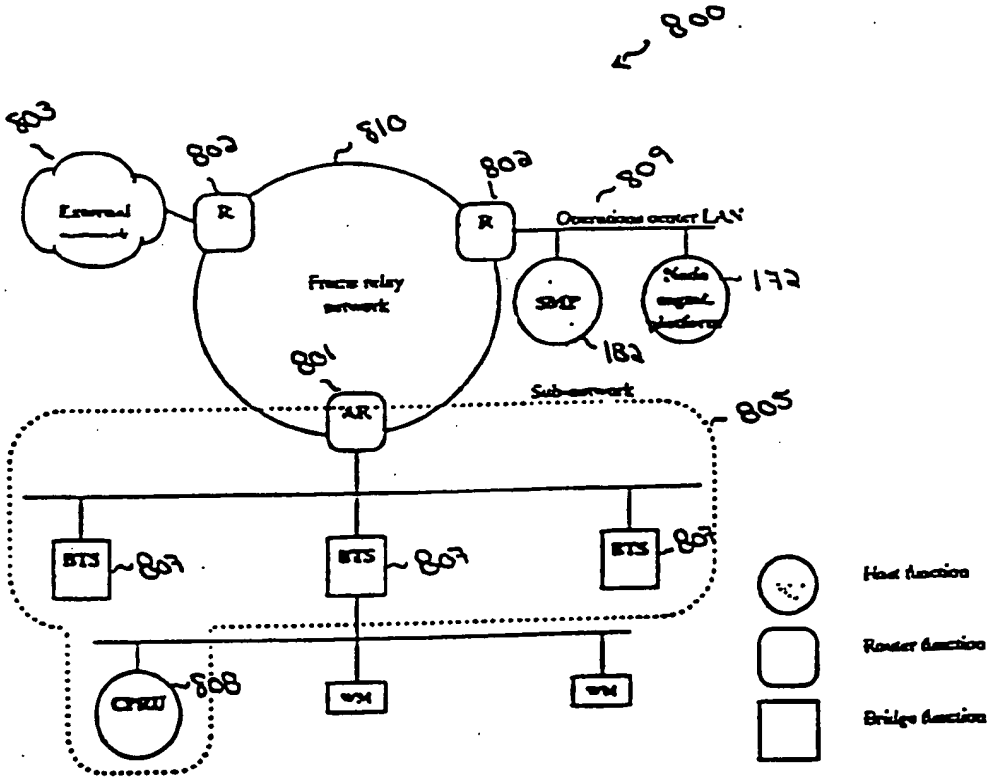

800
803
802
810
802
809
External
R
R
Operations center LAN
Frame relay network
SMF
182
172
801
XR
Subnetwork
805
BTS
807
BTS
807
BTS
807
CPRU
808
WM
WM
Host function
Router function
Bridge function

FIGURE 24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/16791

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :Please See Extra Sheet.
US CL : 370/330, 338, 352, 356, 260, 389

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/330, 338, 352, 356, 260, 389

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 5,796,727 A (HARRISON et al.) 18 August 1998, entire document	1-52
A, P	US 5,905,719 A (ARNOLD et al.) 18 May 1999, entire document	1-52

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
17 AUGUST 1999

Date of mailing of the international search report
15 SEP 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
MICHEAL HORABIK
Telephone No. (703) 305-4704

Form PCT/ISA/210 (second sheet)(July 1992) ☆

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/16791

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (6):

H04L 12/16, 12/66
H04Q 7/00, 7/24